DETERMINACIÓN DEL NIVEL DE INTEGRIDAD DE SEGURIDAD DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD

HOJA DE APROBACIÓN

ELABORA

ING. MANUEL PACHECO PACHECO
COORDINADOR DEL GRUPO DE TRABAJO

PROPONE:

ING. LUIS RAMÍREZ CORZO
PRESIDENTE DEL SUBCOMITÉ TÉCNICO DE NORMALIZACIÓN
DE PEMEX-EXPLORACIÓN Y PRODUCCIÓN

APRUEBA:

ING. RAFAEL FERNÁNDEZ DE LA GARZA
PRESIDENTE DEL COMITÉ DE NORMALIZACIÓN DE
PETRÓLEOS MEXICANOS Y ORGANISMOS SUBSIDIARIOS

México, D. F., a 17 de mayo de 2003.

C O N T E N I D O

0. INTRODUCCIÓN.

Dentro de las principales actividades que se llevan a cabo en Petróleos Mexicanos se encuentra el diseño, construcción, operación y el mantenimiento de las instalaciones para la extracción, recolección, almacenamiento, medición, transporte, procesamientos primario y secundario de hidrocarburos, así como la adquisición de materiales y equipos requeridos, para cumplir con eficacia y eficiencia los objetivos de la empresa. En vista de esto, es necesaria la participación de las diversas disciplinas de la ingeniería, lo que involucra diferencia de criterios.

Para definir los requerimientos en la determinación del Nivel de Integridad de Seguridad (NIS, SIL) para Sistemas Instrumentados de Seguridad (SIS) en instalaciones de Petróleos Mexicanos y Organismos Subsidiarios, es necesaria la participación de las diversas disciplinas de la ingeniería para unificar criterios y aprovechar las experiencias diversas; conjuntando los resultados con las investigaciones nacionales e internacionales. Para ello, Petróleos Mexicanos y Organismos Subsidiarios emiten la presente norma.

Este documento normativo se realizó en atención y cumplimiento a:

Ley Federal sobre Metrología y Normalización.
Ley de Obras Públicas y Servicios Relacionados con las Mismas.
Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Ley General de Equilibrio Ecológico y Protección Ambiental.
Las Reglas Generales para la Contratación y Ejecución de Obras Públicas.
Reglamento de la Ley Federal sobre Metrología y Normalización.
Reglamento de la Ley de Obras Públicas y Servicios Relacionados con las Mismas.
Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Guía para la redacción, estructuración y presentación de las normas mexicanas NMX-Z-13/1-1997.
Guía para la emisión de Normas de Referencia de Petróleos Mexicanos y Organismos Subsidiarios.

En esta norma participaron:

Pemex Exploración y Producción.
Pemex Gas y Petroquímica Básica.
Pemex Refinación.
Pemex Petroquímica.
Petróleos Mexicanos.

Participantes externos:

Instituto Mexicano del Petróleo.
Grupo ARPO.
ICS triplex.
HIMA Américas, Inc.
ABS Group Services de México, S.A. de C.V.
REDCA Red de Capacitación y Servicios Profesionales, S.A. de C.V.
DEMAR Instaladora y Constructora.
DIRESSA Diesel Refacciones y Servicios, S.A. de C.V.
Invensys México/Triconex.
ABB México.
Moore Products.

1. OBJETIVO.

Este documento normativo técnico presenta los requisitos mínimos y metodología que se debe cumplir en la contratación de los servicios para la elaboración de estudios para determinar el nivel de integridad de seguridad de los sistemas instrumentados de Petróleos Mexicanos y Organismos Subsidiarios.

2. ALCANCE.

Esta norma de referencia conforma los requerimientos de diseño para los Sistemas Instrumentados de Seguridad y la metodología para verificar que se cumplan dichos requerimientos en los procesos industriales de las instalaciones petroleras siendo de aplicación y cumplimiento estricto en todas las áreas de Pemex involucradas en el diseño, construcción, operación y mantenimiento.

3. CAMPO DE APLICACIÓN.

Esta norma es de observancia obligatoria en las adquisiciones, arrendamientos o contrataciones de los bienes o Servicios involucrados en el desarrollo y ejecución de proyectos que requieran o involucren Sistemas Instrumentados de Seguridad (SIS) en los procesos de las instalaciones de Petróleos Mexicanos y Organismos Subsidiarios. Por lo que debe ser incluida en los procedimientos de contratación: licitación pública, invitación a cuando menos tres personas, o adjudicación directa, como parte de los requisitos que deben cumplir el proveedor, contratista o licitante.

4. ACTUALIZACIÓN.

Esta norma se debe revisar y en su caso modificarse cada 5 años, ó antes si las sugerencias y recomendaciones de cambio lo ameritan. Las propuestas y sugerencias de cambio deben dirigirse por escrito a:

Pemex Exploración y Producción
Unidad de Normatividad Técnica
Bahía de Ballenas, No. 5, Edificio “D”, 9° piso
Col. Verónica Anzures
11300 México, D.F.
Teléfono directo: 55.45.20.35, Conmutador: 57.22.25.00, Ext. 3.80.80, Fax 3.26.54.
email: mpacheco@pep.pemex.com

5. REFERENCIAS.

5.1 NOM-001-SEDE-1999, Instalaciones Eléctricas.

5.2 IEC 60534-2 Válvulas de control de procesos industriales, Parte 2: Capacidad de flujo, Septiembre 1998 (Industrial Process Control Valves, Part 2: Flow Capacity, September 1998).

5.3 IEC 61508, 2000 Estándar Seguridad Funcional: Sistemas de Seguridad (Functional Safety: Safety Related Systems, IEC Standard 61508, 2000).

5.4 IEC 61131-3 Controladores Programables 1994, Parte 3, Lenguajes de programación (IEC 61131-3 Programmable Controllers 1994, Part 2).

5.5 NRF-011-PEMEX-2001 Sistemas Automáticos de Alarma por Detección de Fuego y/o por Atmósferas Riesgosas (SAAFAR).

6. DEFINICIONES.

6.1 Árbol de fallas. Representación gráfica lógica y organizada de las condiciones ó factores que causan o contribuyen a que ocurra un evento no deseado definido.

6.2 Capas de protección. Sistemas de protección que generalmente involucran diseños especiales, equipo de proceso, sistema de control básico de proceso, procedimientos administrativos, y/o respuestas planeadas para protección contra un riesgo inminente.

6.3 Ciclo de vida de seguridad. Secuencia de actividades involucradas en la implantación de sistemas instrumentados de seguridad desde el diseño conceptual hasta el desmantelamiento del mismo.

6.4 Comisionamiento. Es la verificación y confirmación de que el SIS cumple con las características especificadas en la documentación del diseño detallado y se encuentra listo para las pruebas de prearranque o PAS (OSAT) (ver punto 8.8.1.1).

6.5 Competencia. Tener la destreza necesaria, conocimiento, entendimiento y madurez de juicio para ser capaz de cumplir con las obligaciones de manera segura y efectiva.

6.6 Complejidad. Un indicador del número de grados de libertad al cometer errores.

6.7 Comunicación externa. Intercambio de datos entre el SIS y una variedad de sistemas o dispositivos que se encuentran fuera del SIS. Esto incluye interfases del operador compartidas, interfases de ingeniería/mantenimiento, sistemas de adquisición de datos, entre otros.

6.8 Comunicación interna. Intercambio de datos entre diferentes dispositivos dentro de un SEP (PES) dado. Esto incluye conexiones de plano posterior (back plane) del bus, I/O del bus locales o remotas, entre otros.

6.9 Confiabilidad. Probabilidad de que un sistema pueda desempeñar una función definida bajo condiciones especificadas para un periodo de tiempo dado.

6.10 Demanda. Una condición ó evento que requiere que el SIS lleve a cabo una acción apropiada para prevenir un evento peligroso, ó para mitigar sus consecuencias.

6.11 Desenergizado para disparo. Circuitos SIS en donde las salidas y dispositivos se encuentran energizados en operación normal. Cuando se suspende el suministro de energía se produce una acción de disparo.

6.12 Desmantelamiento parcial. Es un caso particular de modificación, el cual consiste en la remoción de una ó más funciones instrumentadas de seguridad (FIS) del SIS.

6.13 Desmantelamiento. La remoción completa de un SIS de su servicio activo.

6.14 Disparos en falso. Activación de cualquier Función Instrumentada de Seguridad (FIS) perteneciente al SIS, sin existir una demanda real en campo.

6.15 Disponibilidad de seguridad. Fracción de tiempo en que un sistema de seguridad es capaz de desempeñar un servicio de seguridad designado cuando el proceso esta en operación. Un SIS no esta disponible si se encuentra en un estado de falla (seguro o peligroso), o esta fuera para mantenimiento.

6.16 Diversidad. Uso de dispositivos y equipos con diferentes tecnologías o métodos de diseño que desempeñen una función de seguridad común, de manera que se minimicen las fallas de causa común.

6.17 Energizado para disparo. Circuitos SIS en donde las salidas y dispositivos se encuentran desenergizados en operación normal. Cuando a dichos circuitos se les aplica energía se produce una acción de disparo.

6.18 Estado seguro. Estados que debe tener el equipo o proceso bajo control después de la operación apropiada del SIS.

6.19 Falla de causa común. Falla resultado de uno o más eventos, causando fallas coincidentes de dos o más componentes separados conduciendo a la falla del SIS.

6.20 Falla no revelada. Fallas que pueden ser clasificadas como ocultas, encubiertas, no detectadas, latentes, entre otras.

6.21 Falla segura. Es una falla la cuál no tiene el potencial para poner el SIS referido a seguridad en un estado dañino o en un estado de falla para funcionar.

6.22 Falla revelada. Fallas que son clasificadas como anunciadas, detectadas, reveladas, entre otras.

6.23 Fallas sistemáticas. Fallas debido a errores (incluyendo equivocaciones y omisiones) en las actividades del ciclo de vida de seguridad, las cuáles causan que el SIS falle bajo alguna combinación particular de entradas o bajo ciertas condiciones ambientales.

6.24 Filosofía de operación del sistema. Este documento debe contener la narrativa - diagramas lógicos y narrativa - diagramas causa y efecto.

6.25 Función de seguridad. Es una función a ser implantada por un sistema de seguridad.

6.26 Función Instrumentada de Seguridad (FIS). Capa de protección instrumentada independiente, cuyo propósito es llevar al proceso a un estado seguro cuando se violan condiciones predeterminadas.

6.27 Intervalo de prueba. Intervalo de tiempo entre pruebas funcionales.

6.28 Modo degradado. Es aquél estado en el cuál el SIS aún está operando satisfactoriamente pero se encuentra vulnerable con respecto a fallas posteriores.

6.29 Nivel de Integridad de Seguridad (NIS, SIL). Es un nivel discreto para la especificación de los requerimientos de integridad de las funciones de seguridad a ser asignadas a sistemas instrumentados de seguridad. Cada nivel discreto se refiere a cierta probabilidad de que un sistema referido a seguridad realice

satisfactoriamente las funciones de seguridad requeridas bajo todas las condiciones establecidas en un periodo de tiempo dado.

6.30 Probabilidad de Falla en Demanda (PFD). Un valor que indica la probabilidad de que un SIS falle para responder a una demanda.

6.31 Procesador lógico. Sistema o elemento electrónico diseñado para tomar las acciones necesarias sobre la base de una lógica determinada, estos sistemas incluyen módulos de entrada y salida.

6.32 Prueba funcional. Actividad periódica para verificar que el SIS esta en operación de acuerdo a la especificación de los requerimientos de seguridad.

6.33 Prueba en línea. Prueba requerida para confirmar la correcta operación del SIS; esta prueba se debe llevar a cabo si resulta impráctico poner fuera de servicio al equipo bajo control para satisfacer la frecuencia de pruebas requerida. Esta prueba no necesariamente se realiza con el fluido de proceso fluyendo a través de los elementos finales (válvulas) del SIS, ya que puede darse el caso de que se trate de un diseño que haya contemplado algún desvío (by pass) alrededor de la válvula del SIS.

6.34 Prueba integral. En caso de que el SIS forme parte de un proyecto integral en el cual existan otros equipos que tengan una interrelación con el SIS, se realizan las pruebas integrales del SIS que confirmen la funcionalidad correcta del sistema completo, incluyendo la lógica de acuerdo a las especificaciones de los requerimientos de diseño. Esta verificación se realiza después de que las pruebas PAS (OSAT) del SIS han sido completadas de manera satisfactoria

6.35 Redundancia. Uso de elementos o sistemas múltiples, de igual o diferente tecnología, para desempeñar la misma función.

6.36 Redundancia diversa. La redundancia diversa, aplica diferente tecnología, diseños, manufactura, programas de cómputo (software), etc. con la finalidad de reducir la influencia de fallas de causa común. La redundancia diversa debe emplearse únicamente para alcanzar el NIS (SIL) requerido, este tipo de redundancia no debe emplearse cuando su aplicación resulte en el uso de componentes de baja confiabilidad.

6.37 Relé. Relevador. Tecnología usada en Sistemas Instrumentados de Seguridad basada en señales lógicas discretas (encendido/apagado).

6.38 Sensor. Dispositivo o combinación de dispositivos que miden las condiciones del proceso (transmisores, interruptores de proceso, interruptores de posición, entre otros).

6.39 SIS (Safety Instrumented Systems). Es un sistema compuesto por sensores, procesadores lógicos y elementos finales de control que tiene el propósito de llevar al proceso a un estado seguro cuando se han violado condiciones predeterminadas. Otros términos comúnmente usados son Sistema de Paro de Emergencia **SPE (ESD)** y Sistema de Paro de Seguridad.

6.40 Sistemas de seguridad. Es todo aquél sistema que implanta las funciones de seguridad necesarias para mantener un estado seguro en el equipo bajo control.

6.41 Sobre tensión. Aumento grande repentino y transitorio de la corriente o tensión en un circuito o a lo largo de un conductor. Sobre tensión inicial de encendido de un aparato.

6.42 Tasa de demanda. La frecuencia con el cuál un SIS es requerido para realizar su función.

6.43 Tasa de fallas. Es la tasa promedio a la cual se espera que ocurran fallas de los componentes del SIS.

6.44 Tiempo medio de reparación. El tiempo medio para reparar un elemento del SIS. Este tiempo abarca los tiempos involucrados desde que la falla ocurre hasta que la reparación se ha completado y el dispositivo ha regresado a operación normal.

6.45 Tiempo medio de disparo en falso. Tiempo medio para que se presente una falla del SIS que resulta en un paro en falso del proceso o del equipo bajo control.

6.46 Validación. Confirmación por medio de revisión y suministro de evidencia objetiva que los requerimientos particulares para un uso particular y específico son totalmente cumplidos.

6.47 Verificación. Confirmación por medio de revisión y suministro de evidencia objetiva del cumplimiento total de los requerimientos.

7. SIMBOLOS Y ABREVIATURAS.

7.1 ACP. Análisis de Capas de Protección (**LOPA.** Layers of Protection Analyses).

7.2 AMFE. Análisis de Modos de Falla y Efectos (**FMEA.** Failure Modes and Effects Analysis).

7.3 ANSI. Instituto de Estándares Nacionales Americanos (American National Standards Institute).

7.4 CNPMOS. Comité de Normalización de Petróleos Mexicanos y Organismos Subsidiarios.

7.5 FIS. Función instrumentada de seguridad (**SIF.** Safety Instrumented Function).

7.6 FRR. Factor de reducción de riesgo.

7.7 HAZOP. Análisis de Peligro y Operabilidad (Hazard and Operability).

7.8 IEC. Comisión Electrotécnica Internacional (International Electrotechnical Commission).

7.9 IMP. Instituto Mexicano del Petróleo.

7.10 ISA. Sociedad Instrumentista de América (Instrument Society of America).

7.11 $MTTF^{falso}$ Tiempo medio de disparo en falso.

7.12 MTTR. Tiempo medio de reparación.

7.13 NIS. Nivel de Integridad de Seguridad (**SIL.** Safety Integrity Level).

7.14 OREDA. Datos de Confiabilidad Costa fuera (Offshore Reliability Data).

7.15 PAF. Pruebas de Aceptación en Fábrica (**FAT.** Factory Acceptance Test)

7.16 PAS. Prueba de aceptación en sitio (**OSAT.** On Site Acceptation Test).

7.15 **Pemex.** Petróleos Mexicanos y Organismos Subsidiarios.

7.16 **SCBP.** Sistema de Control Básico de Proceso (**BPCS.** Basic Process Control System).

7.17 **SEP.** Sistema Electrónico Programable (**PES.** Programmable Electronic System).

7.18 **SIS.** Sistema Instrumentado de Seguridad (Safety Instrumented System).

7.19 **SPE.** Sistema de Paro por Emergencia (**ESD.** Emergency Shutdown).

7.20 **SUTEN.** Subcomité Técnico de Normalización.

7.21 **UKOOA.** Asociación de operadores costa fuera del Reino Unido (United Kingdom Offshore Operators Association).

8. DESARROLLO.

Los Sistemas Instrumentados de Seguridad son muy importantes en la administración de riesgos debido a que reducen o evitan las consecuencias de los peligros al personal, al ambiente e instalaciones. Los riesgos deben prevenirse como un objetivo inicial del diseño y deben ser mitigados para reducir el riesgo al personal. Por lo tanto, los Sistemas Instrumentados de Seguridad (SIS) cumplen una función primordial evitando los eventos de riesgo o minimizando la severidad de las consecuencias al personal, medio ambiente e instalaciones.

A continuación se presenta de manera introductoria cada uno de los pasos que conforman el ciclo de vida de un Sistema Instrumentado de Seguridad.

8.1 Ciclo de vida de seguridad del SIS.

El ciclo de vida de seguridad debe comprender las actividades para la implantación de los Sistemas Instrumentados de Seguridad (SIS) desde la concepción inicial hasta el desmantelamiento (ver figura 1). Sin embargo, las primeras etapas del ciclo de vida de seguridad sombreadas en la figura 1: Diseño Conceptual del Proceso, Análisis de Peligros de Proceso y Evaluación de Riesgos, y Capas de Protección NO-SIS se encuentran fuera del alcance de la presente norma. Los resultados de estas etapas son los datos de entrada al desarrollo de esta norma, por lo anterior, la eficacia y eficiencia en la aplicación de esta norma dependerá de la confiabilidad y exactitud de dichos datos.

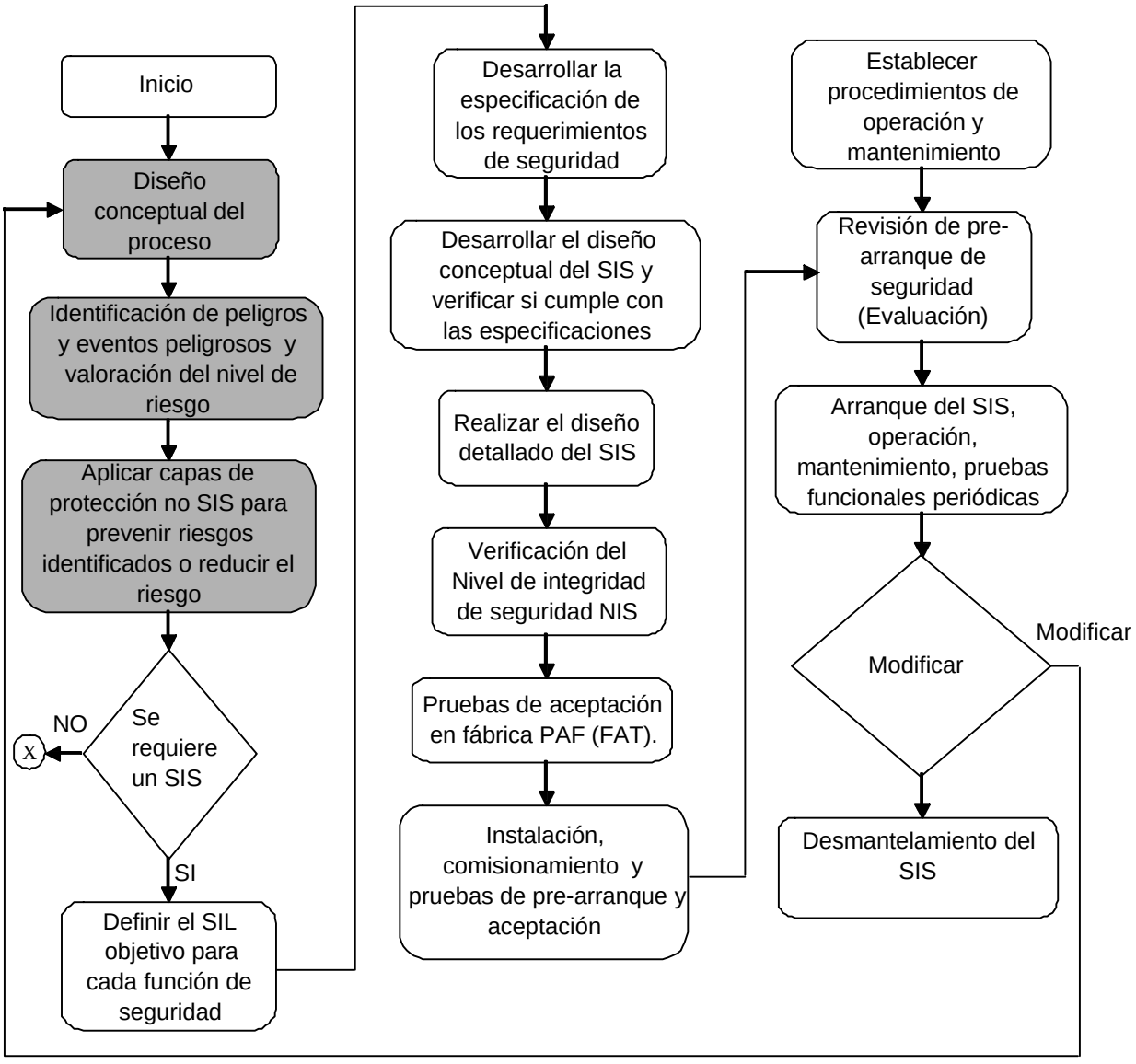


Figura 1. Modelo del ciclo de vida de seguridad (adaptado de 11.12 capítulo 4).

Nota. Las etapas sombreadas se encuentran fuera del alcance de esta norma.

8.1.1 Diseño conceptual de proceso.

En esta primera etapa del ciclo de vida de seguridad del SIS y para el caso de esta norma se debe contar con un diseño conceptual del proceso incluyendo las filosofías de operación, el equipo de proceso y el sistema básico de control del proceso, tomando en consideración las condiciones ambientales del lugar.

8.1.2 Identificación de peligros y eventos peligrosos para un proceso y la valoración del nivel de riesgo involucrado.

Para el buen desarrollo de esta norma, se debe de contar con un análisis y evaluación de riesgos. Dicho análisis y evaluación de riesgos se deben llevar a cabo tanto en los procesos de instalaciones nuevas como existentes, que sufran modificaciones en su proceso o en los que no cuenten con dichos análisis. Se debe considerar el riesgo sobre el personal, medio ambiente, producción, equipo e imagen corporativa de la empresa. El objetivo de un análisis de riesgo es la identificación de riesgos de proceso, una vez identificados los mismos, se lleva a cabo su valoración (frecuencia/consecuencia) y posteriormente se debe decidir si ese riesgo es tolerable o no basándose en los criterios de aceptación del riesgo específico para el sistema y/o instalación definidos por Pemex. Para reducir el riesgo a un nivel tolerable, primero deben de aplicarse capas de protección NO-SIS, en caso de no alcanzar el nivel de riesgo tolerable una vez aplicadas dichas capas, se requiere implantar un sistema instrumentado de seguridad, para lo cual se continúa con la siguiente etapa del ciclo de vida (11.23, capítulo 1). Los resultados del análisis de riesgo deben constituir los datos de entrada para la determinación del NIS (SIL) objetivo, por esta razón deben ser obtenidos de un análisis cuantitativo que considere el análisis de capas de protección adicionales o bien mediante un análisis LOPA (ACP).

8.1.3 Aplicación de capas NO SIS.

El objetivo del diseño de proceso es obtener una planta inherentemente segura, en dónde los riesgos residuales puedan ser controlados mediante la aplicación de capas de protección no instrumentadas. La reducción del riesgo mediante la selección cuidadosa de los parámetros operacionales básicos del proceso constituye una pieza clave en el diseño de un proceso seguro. Sin embargo, aún después de aplicar esta filosofía de diseño pueden permanecer riesgos potenciales, por lo cuál es necesario aplicar medidas de protección adicionales para controlar dichos riesgos. Cada capa de protección adicional consiste de un conjunto de equipos y/o controles administrativos, los cuáles interactúan con otras capas de protección controlando de esta manera el riesgo. Una vez que ha sido seleccionado el proceso básico, el diseño de proceso detallado proporciona el primer nivel de protección. Posteriormente, el sistema de control básico de proceso en conjunción con la supervisión del operador, el sistema de alarmas y las acciones correctivas iniciadas por el operador proporcionan otras capas adicionales de protección (11.1).

El método (ACP-LOPA) debe cumplir con las siguientes características:

a) Identificar los eventos iniciadores de impactos indeseados, determinando el tipo de impacto (al ambiente, al personal, a las instalaciones).
b) Listar las causas de cada impacto.
c) Estimar las frecuencias de cada evento iniciador.
d) Listar las capas de protección diseñadas o existentes.
e) Determinar la probabilidad de falla en demanda de cada capa de protección.
f) Calcular la frecuencia de todas las rutas que se originan desde el evento iniciador, multiplicando la frecuencia del evento iniciador por cada una de las probabilidades que apliquen.
g) Comparar la frecuencia final de resultados indeseados contra el criterio de riesgo tolerable. Si no se cumple con dicho criterio, entonces adicionar capas de protección.

8.1.4 Criterios para determinar la necesidad de un Sistema Instrumentado de Seguridad (SIS):

Si los riesgos pueden ser controlados a un nivel aceptable (ver tabla 1 de frecuencias objetivo) sin la aplicación de un Sistema Instrumentado de Seguridad, entonces la etapa de diseño de proceso finaliza. Si los riesgos por el contrario no pueden ser controlados a un nivel aceptable mediante la aplicación de capas de seguridad no instrumentadas, entonces se requerirá un Sistema Instrumentado de Seguridad (SIS) y el ciclo de vida de

seguridad continúa a la siguiente etapa. Cuando ocurre una falla en las capas de protección del proceso y del sistema de control básico de proceso y el control del riesgo no puede ser llevado a un nivel aceptable, se requiere la instalación de un Sistema Instrumentado de Seguridad (SIS) que lleve a cabo medidas que controlen el riesgo dentro de un nivel aceptable (11.23 capítulo 1).

8.1.5 La definición del Nivel de Integridad de Seguridad Objetivo (NIS, SIL).

La siguiente etapa consiste en establecer los requerimientos para el SIS definiendo un nivel de integridad de seguridad objetivo (NIS, SIL objetivo). El NIS (SIL) debe definir el nivel de desempeño en la operación necesario para lograr el objetivo de seguridad de proceso del usuario. Para industrias de proceso se consideran tres diferentes niveles (1, 2 y 3) y se categorizarán sobre la base de probabilidades de falla en demanda/factor de reducción del riesgo. Este asunto se presenta de una manera más explícita en el punto 8.2.

8.1.6 Especificación de los requerimientos de diseño.

En este paso el contratista debe desarrollar la especificación de los requerimientos de seguridad, esencialmente la filosofía de operación del sistema. Cada función de seguridad debe tener un requerimiento de NIS (SIL) asociado y requerimientos de confiabilidad para disparos en falso. Se deben incluir todas las condiciones de operación del proceso, desde el arranque hasta el paro, incluyendo el mantenimiento para cada modo de operación del proceso. Este asunto se presenta de una manera más explícita en el punto 8.3.

8.1.7 Diseño conceptual del SIS.

En esta etapa, el contratista debe desarrollar un diseño inicial para verificar si se cumple con los requerimientos de seguridad y de operación del NIS (SIL) Se debe inicialmente seleccionar una tecnología, configuración (arquitectura), intervalo de prueba, entre otros. Posteriormente debe proceder la verificación cuantitativa para ver si el sistema propuesto cumple los requerimientos de operación. Este asunto se presenta de una manera mas explícita en el punto 8.4.

8.1.8 Diseño detallado del SIS.

El propósito de la etapa del diseño detallado es finalizar y documentar el diseño conceptual. Una vez que se ha elegido un diseño, el sistema debe ser construido siguiendo procedimientos estrictos y buenas prácticas de ingeniería, para evitar errores en el diseño e implantación. En esta etapa el sistema debe ser programado y probado de acuerdo a la lógica determinada, cualquier error cometido durante esta etapa influirá en el resto del diseño (11.23 capítulo 1). Este asunto se presenta de una manera más explícita en el punto 8.6.

8.1.9 Verificación del NIS (SIL)

En esta etapa debe verificarse que cada uno de los elementos que constituyen el diseño propuesto del SIS cumplen con el NIS (SIL) objetivo.

La operación del sistema instrumentado de seguridad (SIS) se basa en un nivel de integridad de seguridad objetivo NIS (SIL) que debe ser definido durante el desarrollo de la especificación de los requerimientos de seguridad.

La habilidad del SIS de lograr un NIL (SIL) especifico debe ser validada en cada etapa de diseño y previo a cualquier cambio realizado al diseño después de la puesta en servicio.

El contratista debe implantar un proceso de validación del NIS (SIL) para asegurar que el SIS cumple con la integridad para cada función de seguridad, para entender la interacción de todas las funciones de seguridad y

para entender el impacto de la falla de cada componente sobre el SIS. Este asunto se presenta de una manera más explícita en el punto 8.5.

8.1.10 Pruebas de Aceptación en Fábrica PAF (FAT).

En esta etapa el sistema debe ser completamente probado antes de ser enviado por el proveedor al usuario final (Pemex).Todos los individuos involucrados con la construcción y la verificación del sistema bajo prueba deben participar en las pruebas PAF (FAT). Estas pruebas deben ser completadas en el sitio de fabricación previo al envío al usuario final, debe probarse tanto el hardware como el software que se está suministrando.

El sistema debe ser revisado y probado en un ambiente controlado, de manera que cualquier problema pueda ser resuelto y corregido usando los recursos disponibles en el sitio del proveedor. Las pruebas PAF (FAT) deben incrementar el entendimiento del personal de diseño y deben aclarar y rectificar cualquier duda. Este asunto se presenta de una manera más explícita en el punto 8.7.

8.1.11 Instalación y comisionamiento.

En esta etapa, el contratista debe asegurar que el sistema sea instalado de acuerdo al diseño y opere de acuerdo a la especificación de los requerimientos de seguridad. Antes de que el sistema sea llevado al sitio debe ser probado hasta su correcta operación, una vez en el sitio, el contratista debe verificar que el sistema esté de acuerdo al diseño detallado incluyendo los dispositivos de campo (comisionamiento). Así mismo deben de llevarse a cabo las pruebas de prearranque y aceptación del sistema por parte de Pemex. El prestador de servicio debe elaborar un procedimiento que dicte los pasos a seguir para la instalación detallada y cada función y etapa deben ser verificadas y documentadas (11.23 capítulo 1). Este asunto se presenta de una manera más explícita en el punto 8.8.1.

8.1.12 Operación y mantenimiento.

El propósito de esta etapa es que el contratista asegure que el sistema funcione correctamente de acuerdo al diseño original y se mantenga durante todas las etapas del ciclo de vida de seguridad, asegurando con esto que responderá efectivamente en caso de una demanda real. La frecuencia de inspección y prueba se determina en una etapa anterior en el ciclo de vida. Toda prueba o inspección debe documentarse y entregarse a Pemex. Este asunto se presenta de una manera más explícita en el punto 8.8.2.

8.1.13 Modificaciones.

Conforme existan cambios en las condiciones del proceso será necesario realizar cambios al sistema de seguridad. Todos los cambios propuestos requieren de un retorno al inicio del ciclo de vida de seguridad. Por lo tanto, el contratista debe proporcionar un procedimiento y registro de implantación formal para el control y evaluación de cambios al sistema y Pemex darle un seguimiento al mismo. Este asunto se presenta de una manera más explícita en el punto 8.8.2.4.

8.1.14 Desmantelamiento.

El desmantelamiento de un SIS debe seguir un proceso de revisión para garantizar que la remoción del servicio de dicho sistema no impacte al proceso o unidades circundantes y que existan los medios necesarios para proteger al personal, equipo y ambiente durante el desarrollo del desmantelamiento (11.23 capítulo 1). Este asunto se presenta de una manera más explícita en el punto 8.9.

8.2 Definir el Nivel de Integridad de Seguridad Objetivo (NIS, SIL).

La determinación del nivel de integridad de seguridad objetivo (NIS, SIL objetivo) de una instalación o sistema debe ser definido con base a un previo análisis cuantitativo de riesgo el cual puede ser realizado por el contratista que diseñe el SIS o por otro, ya que el nivel de integridad determinado está en función de la confiabilidad y exactitud de los resultados de dicho análisis. Un problema potencial con los métodos cualitativos es que sus resultados frecuentemente son subjetivos y no reproducibles, es decir, diferentes organizaciones pueden revisar el mismo proceso y proporcionar requerimientos de (NIS, SIL) muy diferentes entre sí. El contratista debe determinar el nivel de integridad de seguridad (NIS, SIL) para cada función de seguridad y no debe determinarse de manera global para un proceso o instalación, pues esto implicaría considerar los extremos superior e inferior en los valores asignados del NIS (1 ó 3) y se tendría como resultado deficiencias si el (NIS, SIL) objetivo es bajo o bien, una sobre especificación si se establece un (NIS, SIL) alto en el diseño del SIS (11.15).

Para establecer el nivel requerido de integridad del sistema de seguridad se deben considerar los siguientes parámetros (ver punto 10.1 parte 5):

a) La severidad de las consecuencias si el sistema de seguridad falla al operar en demanda.
b) La probabilidad de que el personal sea expuesto al riesgo.
c) Medidas de mitigación para reducir las consecuencias del evento de riesgo.
d) La frecuencia con la cuál el sistema de seguridad se requiere que actúe.

El propósito de seleccionar un (NIS, SIL) objetivo es especificar la reducción de riesgo requerida, es decir, la diferencia entre los niveles de riesgo existente y tolerable, en términos de (NIS, SIL). Para la aplicación de esta etapa, se debe tener definido el nivel de riesgo tolerable para las instalaciones de Pemex y organismos subsidiarios basándose en un análisis cuantitativo de riesgo previo.

Existe un factor en común, independientemente de la naturaleza del método a utilizar, el cuál debe ser considerado no importando el método a emplear esto es, la evaluación de dos componentes del riesgo (la probabilidad del evento de peligro y la severidad de la consecuencia).

La asignación del (NIS, SIL) objetivo se debe realizar basándose en un proceso que lleve el riesgo del proceso a un nivel tolerable.

El proceso de asignación del (NIS, SIL) objetivo (11.15 capítulo 2) debe realizarse empleando el método de frecuencias objetivo. Dicho procedimiento se basa en la selección de la frecuencia objetivo en función de la severidad de las consecuencias obtenidas del análisis de riesgo cuantitativo mediante el uso de la tabla 1.

Nivel de impacto del evento	Consecuencia	Frecuencia objetivo por año
Menor	Impacto inicialmente limitado a un área local del evento con un potencial para una consecuencia más amplia si no se toman acciones correctivas. Fugas dentro de barreras de contención cuyas consecuencias al ambiente son conocidas (ruido, olores e impacto visual detectable, derrame externo controlable en un día)	1.0×10^{-3}
Serio	Es aquélla consecuencia que podría causar cualquier lesión o fatalidad seria en el sitio o fuera de él, o bien, daño a la propiedad de $ 1 MM en el sitio y de $ 5 MM fuera de él. Fugas fuera de los límites sin efectos adversos (el derrame externo se puede controlar en pocos días)	1.0×10^{-4}
Catastrófico	Es aquélla consecuencia que es 5 o más veces severas que un accidente SERIO. Fuga fuera de los límites de contención con efectos adversos (derrame no controlable en pocos días)	1.0×10^{-6}

Tabla 1. Frecuencias objetivo

Una vez definidas las frecuencias objetivo se procede a calcular la reducción del riesgo requerida para cada una de las frecuencias, la cuál es una función de la frecuencia del evento no mitigado y de la frecuencia objetivo:

$$^{obj}PFD_{prom} = F_{objetivo} / F_{evento}$$

En dónde:

$^{obj}PFD_{prom}$ = Probabilidad objetivo de falla en demanda promedio.

$F_{objetivo}$ = Frecuencia objetivo.

F_{evento} = Frecuencia del evento no mitigado.

La asignación del (NIS, SIL) se hace basándose en la PFD requerida (tabla 2). La PFD objetivo se expresa en términos de (NIS, SIL) sobre la base de la tabla especificada por ISA S84 (11.4 parte 1) y IEC 61511(ver punto 10.1 parte 5). Él (NIS, SIL) seleccionado debe proporcionar una mayor reducción de riesgo (FRR) de lo requerido.

Si la PFD calculada para cada una de las frecuencias objetivo es mayor que 10^{-1}, no se requiere un SIS. Si se cumplen ambas condiciones (PFD y FRR) es posible realizar la asignación de (NIS, SIL) correspondiente de acuerdo con la tabla 2:

(NIS, SIL)	PFD	FRR
1	$10^{-1} > PFD > 10^{-2}$	10 - 100
2	$10^{-2} > PFD > 10^{-3}$	100 - 1000
3	$10^{-3} > PFD > 10^{-4}$	1000 - 10000

Tabla 2. Asignación del (NIS, SIL) sobre la base de PFD y FRR.

El método cuantitativo se debe aplicar siempre, sin embargo, Pemex tendrá la opción de solicitar la verificación de los resultados por medio del método cualitativo (ver punto 10.1) si a su criterio el NIS (SIL) objetivo propuesto no satisface los requerimientos de su sistema.

8.3 Especificación de los requerimientos de seguridad.

Una vez determinado que se requiere un Sistema Instrumentado de Seguridad (SIS) y establecido el NIS (SIL) objetivo para cada función de seguridad, el prestador de servicio debe desarrollar y/o aplicar según le corresponda las especificaciones de los requerimientos de diseño para el sistema conforme a las restricciones que Pemex imponga (11.23 capítulo 5). Para tal efecto el contratista y Pemex deben desarrollar la matriz de paro de emergencia, conforme al formato A.1 mostrado en el punto 12.1. Los requerimientos del SIS deben ser expresados y estructurados, de tal modo que sean claros, precisos, verificables, sostenibles, factibles y escritos de modo que puedan ser comprendidos y aplicados. La especificación de los requerimientos de diseño para el SIS debe incluir (11.12 capítulo 5):

a) La función del sistema o componente del sistema.
b) Acciones que el sistema o componente debe realizar bajo circunstancias establecidas (especificación funcional).
c) Integridad requerida (confiabilidad y disponibilidad) para operar en dichas circunstancias (especificación de integridad).
d) Requerimientos de sobrevivencia una vez que un incidente mayor ha sucedido (especificación de sobrevivencia).

La información requerida para el desarrollo de la especificación de los requerimientos de seguridad, debe incluir (11.12 capítulo 5):

a) Lista de las funciones instrumentadas de seguridad requeridas y el NIS (SIL) de cada función de seguridad.
b) Diagramas de proceso e instrumentación, hojas de datos de proceso.
c) Información del proceso (filosofía de operación, elementos finales, entre otros) e información del análisis cuantitativo de riesgo (causa y secuencia de cada evento potencial de peligro que requiera un SIS).
d) Consideraciones de falla de causa común del proceso tales como corrosión, taponamiento, etc.
e) Requerimientos regulatorios que impactan al SIS.
f) Consideraciones de confiabilidad, calidad y ambientales.
g) Lista de consideraciones operacionales y de mantenimiento.

8.3.1 Especificación funcional.

Los requerimientos funcionales deben describir las características de cada función instrumentada de seguridad (FIS). La especificación funcional debe incluir la definición de los parámetros relevantes tales como (ver punto 10.1 parte 1, capítulo 6):

a) Rango de operación normal de las variables del proceso y sus límites máximo y mínimo.
b) El estado seguro del proceso, para cada uno de los eventos identificados.
c) Las entradas de proceso al SIS y sus acciones.
d) Las salidas de proceso del SIS y sus acciones.
e) Interfases e interacciones con otros sistemas (incluyendo el sistema de control básico de proceso y operadores).
f) Punto de referencia (setpoint) de las variables del proceso y su tolerancia.
g) La relación funcional entre la detección y actuación de los elementos finales (entradas y salidas del proceso), incluyendo la lógica, las funciones matemáticas y cualquier otro permisivo que se requiera mediante las representaciones de diagramas lógicos y diagramas causa-efecto.
h) Selección de los modos de energizar o desenergizar para disparo. Generalmente las aplicaciones SIS se encuentran normalmente en el modo energizado y son desenergizadas para disparo. Cuando el proceso específico requiera que alguna aplicación SIS sea normalmente desenergizada y energizada para disparo deberá fundamentarse y demostrarse.
i) Consideraciones para disparo manual.
j) Las acciones a tomar en caso de pérdida de la(s) fuente(s) de energía del SIS.
k) La Respuesta de acción a cualquier falla detectada.
l) Requerimientos de interfase humano-máquina.
m) Funciones de restablecimiento del SIS después de un paro.
n) Los tiempos de respuesta y las tolerancias permisibles de las funciones y de los componentes relevantes.
o) Si la función de seguridad es aplicable a sistemas instrumentados de seguridad operando en modos de operación de baja demanda (no mayor a una demanda por año y una frecuencia de prueba no mayor a 2 veces por año), o de alta demanda/ continua (mayor a una demanda por año y una frecuencia de prueba mayor a dos veces por año).
p) Los modos de operación relevantes del equipo bajo control, lo cuál debe incluir: arranque automático, y manual, semiautomático; estado estacionario, estado estacionario de no operación, reestablecimiento, paro, mantenimiento, y la identificación de las funciones instrumentadas de seguridad requeridas para operar dentro de cada modo.

q) La importancia de las interacciones de los componentes físicos del sistema (hardware)/programas de cómputo (software), e identificar y documentar cualquier restricción para dichas interacciones. Ver punto 8.6.2.
r) Cualquier requerimiento específico referente a los procedimientos de arranque y reestablecimiento del SIS.

8.3.2 Especificación de integridad.

Los requerimientos de integridad, es decir, el nivel de integridad de cada función de seguridad del SIS debe ser usados para establecer una arquitectura aceptable del sistema para lograr el nivel de desempeño, seguridad e integridad requerida para que el SIS ejecute las funciones necesarias. Los requerimientos de integridad de seguridad deben incluir una definición de los siguientes parámetros de integridad (ver punto 10.1 parte 1, capítulo 6):

a) La tasa de demanda supuesta para cada una de las funciones de seguridad.
b) Una descripción de todas las funciones instrumentadas de seguridad para lograr la seguridad funcional requerida y el NIS (SIL) para cada una de ellas.
c) El factor de reducción de riesgo (FRR) para cada función de seguridad.
d) Requerimientos de diagnóstico para lograr el NIS (SIL) requerido.
e) Requerimientos de mantenimiento y prueba para lograr el NIS (SIL) requerido (intervalo mínimo de prueba).
f) Requerimientos de confiabilidad en caso de presentarse disparos en falso (máxima tasa de disparo en falso permisible).
g) Detallar todos los modos requeridos de comportamiento del SIS, particularmente ante fallas y la respuesta requerida (por ejemplo, alarmas, paro automático, entre otros).
h) Las condiciones ambientales extremas probables a ocurrir durante todo el ciclo de vida de seguridad del SIS. Se deben considerar como mínimo las siguientes variables: temperatura, humedad, contaminantes, interferencia electromagnética/interferencia de frecuencia, vibración, descarga electrostática, inundación, clasificación eléctrica de áreas. La interferencia electromagnética se refiere al fenómeno electromagnético no deseado que afecta las señales eléctricas a una banda menor que la radiofrecuencia. Es una forma de ruido eléctrico que surge generalmente de motores, transformadores, conductores de energía y de prácticas de cableado inapropiadas. A su vez, la interferencia por radiofrecuencia surge de señales en falso en el rango de radiofrecuencia (generalmente de 0.5 a 500 MHz), puede generarse de manera local por sistemas de ignición, dispositivos de comunicación de dos vías, equipo de soldadura, dispositivos de control, computadoras, entre otros (11.14).
i) Los límites de inmunidad electromagnética requeridos para lograr compatibilidad electromagnética, los cuáles deben ser fijados considerando tanto el ambiente electromagnético como los niveles de integridad de seguridad requeridos.
j) La iniciación manual de funciones protectoras sustituye en muchos casos a la iniciación automática, por esta razón es importante en funciones iniciadas manualmente considerar la confiabilidad humana, ya que la integridad de los componentes físicos (hardware) de la iniciación manual no debe ser menor a aquélla de la iniciación automática.

8.3.3 Especificación de sobrevivencia.

Las especificaciones de sobrevivencia se refieren al requerimiento específico de que un Sistema Instrumentado de Seguridad permanezca funcionando durante o después de un incidente mayor y son identificadas en la evaluación de riesgos. Si se requiere por parte de Pemex, dichas especificaciones formarán parte de los estándares de desempeño. Una especificación de sobrevivencia será normalmente requerida por válvulas del Sistema Instrumentado de Seguridad y de alivio en áreas de proceso en dónde el actuador y la válvula puedan

ser vulnerables a explosión por sobrepresión externa, fuego, caída de objetos y cualquier otro daño que lo inhabilite antes de que la válvula regrese completamente a su posición segura (11.16 capítulo 4).

8.3.4 Integración de la información y documentación.

La especificación constituye la guía para definir los requerimientos de diseño, por esta razón, se debe incluir toda la información requerida como un paquete completo. Además de la información requerida en el punto 8.3, debe incluirse la siguiente información para integrar el paquete de documentos de la especificación funcional, de integridad y de sobrevivencia (11.23 capítulo 5):

a) Diagramas causa-efecto: También conocidos como matrices de causa efecto para muchos MCF (cause and effects Matrix "CEM") se ha convertido en una herramienta muy familiar para documentar los requisitos de seguridad de un SIS - es una manera muy intuitiva de representar la lógica. Una descripción detallada se puede encontrar en la Norma ISO-10418 de la industria petrolera Estos diagramas se usan para documentar los requerimientos funcionales y de integridad. Deben ser documentos claros para todas las disciplinas, ver figura 2.
b) Diagramas lógicos: Estos diagramas se deben usar en adición de los diagramas causa-efecto para funciones complejas y basadas en tiempo, así como para secuencias complejas que no pueden ser descritas fácilmente mediante un diagrama de causa-efecto.

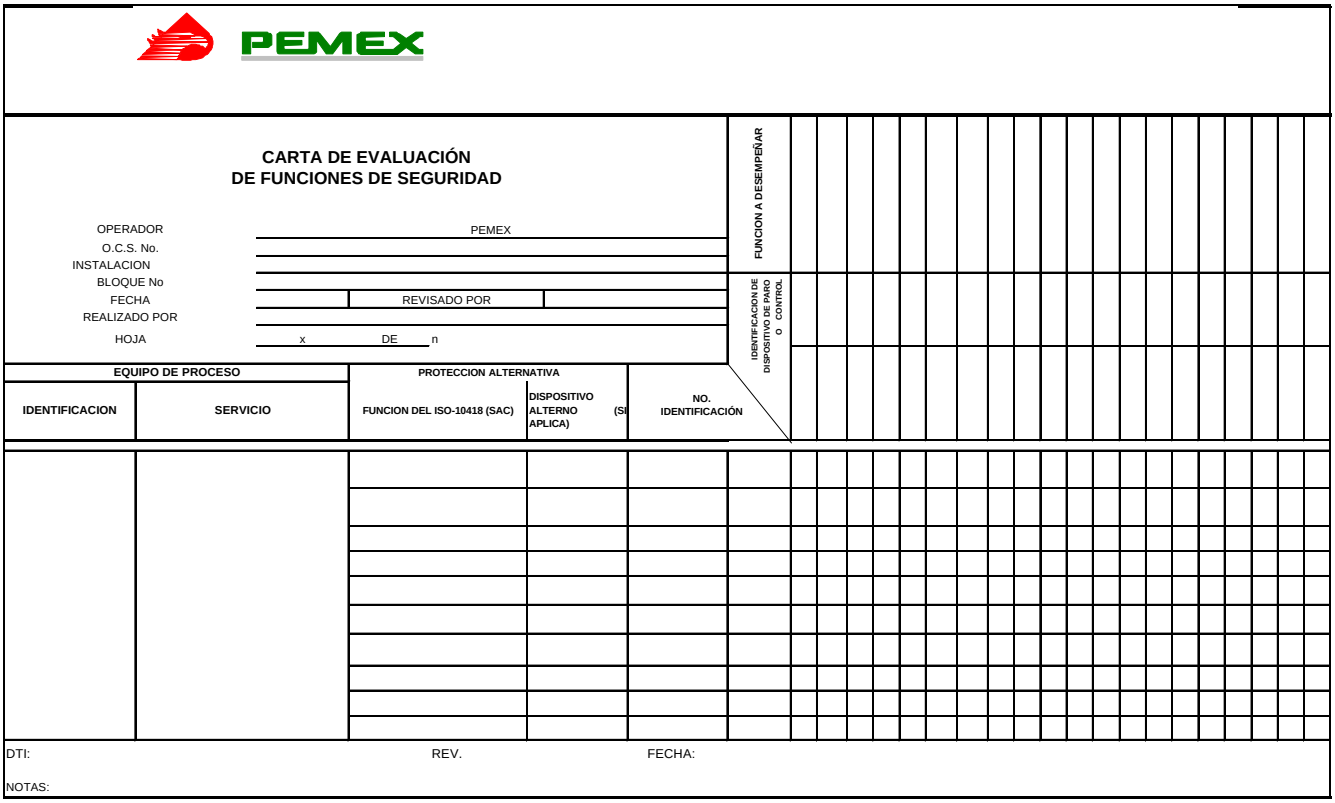


Figura 2. Ejemplo de un diagrama de causa - efecto típico.

La especificación debe de establecer lo que se va a lograr y no necesariamente de qué manera se va a lograr. El método para documentar las especificaciones de los requerimientos de seguridad debe ser lo suficientemente simple para lograr un buen entendimiento del mismo (11.23 capítulo 5).

Una vez terminada la especificación de los requerimientos de seguridad, debe ser revisada y aprobada por Pemex. Una vez aprobada la especificación no deben existir cambios a menos que estén debidamente justificados y aprobados por Pemex. La especificación debe de llevar el registro del número de revisión correspondiente cuando se realicen cambios durante el curso del proyecto.

8.4 Consideraciones de diseño conceptual del SIS.

El propósito del diseño conceptual es definir las características técnicas para la realización y mantenimiento bajo estándares de los Sistemas Instrumentados de Seguridad SIS. Los sistemas de protección deben estar constituidos de los siguientes elementos (11.16 capítulo 5):

a) Elementos primarios.
b) Sistemas eléctricos, electrónicos o electrónicos programables.
c) Elementos finales.
d) Hardware y software adicionales necesarios para el correcto funcionamiento del SIS.

8.4.1 Independencia del SIS con otros sistemas.

La separación del sistema de control básico de proceso SCBP (BPCS) y las funciones del Sistema Instrumentado de Seguridad SIS reducen la probabilidad de que el control y las funciones de seguridad no estén disponibles al mismo tiempo, ya que cambios inadvertidos afectarían la funcionalidad de seguridad del SIS. Debe existir una separación total entre estos dos sistemas, en casos donde no sea posible separar dichos sistemas en un proceso o equipo especifico y contratista se debe fundamentar y demostrar que no se compromete la integridad de las funciones de seguridad.

La separación Idéntica, debe constar de dos o más unidades o componentes idénticos e independientes entre si. La separación diversa debe constar de dos o más unidades o componentes diferentes (con diferente tecnología, configuración, entre otros factores) e independientes entre sí, además este tipo de separación reduce la probabilidad de fallas sistemáticas y las fallas de causa común.

La separación debe considerarse y evaluarse para cumplir con la funcionalidad de seguridad y los requisitos de integridad en las siguientes áreas:

a) Aplicación a sensores de campo.
b) Aplicación a elementos finales de control.
c) Procesador lógico.
d) Comunicación entre SIS y el sistema de control básico de proceso SCBP (BPCS) u otro equipo.

Sensores de campo. Para NIS (SIL) 1 y NIS (SIL) 2, es necesaria la separación idéntica entre el sistema de control básico de proceso SCBP (BPCS) y el SIS para alcanzar la integridad de seguridad requerida.

Para NIS (SIL) 3, la separación puede ser idéntica o diversa entre el sistema de control básico de proceso SCBP (BCPS) y el SIS para cumplir con la integridad de seguridad requerida.

Válvulas de cierre y control. Para NIS (SIL) 1, puede usarse una sola válvula para ambos sistemas SCBP (BPCS) y SIS, con la condición de que la tasa de falla, cumpla los requisitos de integridad de seguridad. El diseño debe asegurar que las acciones del SIS prevalezcan sobre las acciones del SCBP (BPCS).

Para NIS (SIL) 2, se requiere la separación idéntica entre SCBP(BPCS) y SIS, para cumplir el nivel de integridad de seguridad requerida. El uso de una sola válvula para SCBP (BPCS) y SIS requiere un análisis y revisión de seguridad, ya que de lo contrario puede no cumplirse la integridad de seguridad requerida.

Para NIS (SIL) 3, la separación debe ser idéntica o diversa entre el SCBP (BPCS) y SIS para alcanzar la integridad de seguridad requerida.

Consideraciones adicionales para determinar los requisitos de una válvula son:

a) Los requerimientos de corte.
b) La experiencia de confiabilidad con la válvula.
c) Los modos de falla de la válvula.
d) Procedimientos operativos que contribuyan a que la válvula sea menos efectiva.

Procesador lógico. Para NIS (SIL) 1, la separación entre el sistema de control básico de proceso SCBP (BPCS) y SIS debe ser idéntica o diversa para lograr la integridad de seguridad requerida.

Para NIS (SIL) 2, se requiere separación diversa entre el sistema de control básico de proceso SCBP (BPCS) y el SIS para cumplir con la integridad de seguridad requerida.

Para NIS (SIL) 3, debe existir una separación diversa entre el sistema de control básico de proceso SCBP (BPCS) y el SIS para cumplir con la integridad de seguridad requerida.

Existen casos especiales dónde no es posible separar el sistema de control básico de proceso SCBP (BPCS) del SIS. Algunas consideraciones mínimas para estos casos especiales son:

a) Evaluación de las fallas de los componentes comunes y programas de cómputo (software) y su impacto en el desempeño del SIS.
b) El ciclo de vida debe soportar al sistema completo como un SIS con respecto a los cambios, mantenimiento, pruebas, y documentación.
c) Limitar el acceso a la programación o la configuración de las funciones del sistema.

Las comunicaciones entre el sistema de control básico de proceso SCBP (BPCS), el sistema de gas y fuego y el SIS. (ver NRF-011-PEMEX-2001 Sistemas Automáticos de Alarma por Detección de Fuego y/o por Atmósferas Riesgos (SAAFAR).

En algunos casos se requiere comunicación entre el sistema de gas y fuego y el SIS para reforzar la seguridad global. En el caso de el sistema de gas y fuego y el SIS es bidireccional, sin embargo entre el SIS y el SCBP (BPCS) debe ser unidireccional con comunicación únicamente del SIS hacia el SCBP (BPCS). Las formas básicas de comunicación externa entre SCBP (BPCS) y el SIS aceptadas por esta norma son:

1) No hay comunicación externa del SCBP (BPCS) al SIS. Esto es aplicable para todos los NIS's (SILs), pero si hay comunicación entre el SIS y el sistema de gas y fuego.
2) Comunicación por cable entre el SCBP (BPCS) y el SIS, esto es aceptable para NIS (SIL) 1 y NIS (SIL) 2, pero el uso de este método para NIS (SIL) 3 requiere análisis y revisiones de seguridad adicionales.

3) Sólo lectura en la comunicación externa del SIS al SCBP (BPCS). Esto tipo de comunicación es aceptable para todos los NIS (SIL) siempre y cuando la revisión y el análisis asegure que no se compromete a la función de seguridad. Las medidas para protección de la escritura de la función de seguridad deben incluir:
   a) Contraseña (password) para limitar el acceso a la escritura.
   b) La aplicación de la función de seguridad del SIS en memoria de solo lectura ROM (Read Only Memory).
4) Comunicaciones externas lectura/escritura con protección a la escritura de la función de seguridad. Este tipo de comunicación es aceptable para NIS (SIL) 1 y 2, pero el uso de este método para NIS (SIL) 3 requiere análisis y revisiones adicionales de seguridad. Las medidas para lograr protección a la escritura de la función de seguridad deben incluir:
   a) Un límite de tiempo para acceder a la escritura.
   b) Un interruptor de los programas de cómputo (software), por ejemplo, una contraseña, para limitar el acceso a la escritura.
5) Comunicación externa de lectura/escritura con protección limitada o sin protección a la escritura de la función de seguridad. El uso de este método es aceptable para NIS (SIL) 1. El Uso de este método para NIS (SIL) 2 requiere análisis y revisiones de seguridad adicionales. No se debe usar de este método para NIS (SIL) 3.

8.4.1.1 Sistema de control de procesos (11.16 capítulo 5). Este sistema es muy importante en la determinación de la tasa de demanda de los sistemas de protección. Debe minimizarse la probabilidad de que cualquier falla simple en el sistema de control lleve a una demanda del SIS. Todos los modos de fallas previsibles deben ser identificados de modo que se consideren en el diseño del sistema de protección.

En instalaciones de producción se pueden implantar funciones protectoras poco críticas (en base al análisis de riesgos) en el sistema de control de proceso siempre que se cumpla que la integridad de seguridad no sea tan elevada como para implantar un SIS en áreas en las cuales es más que suficiente el sistema de control de procesos, de otro modo el sistema de control debe ser diseñado como un sistema de seguridad.

La comunicación del SIS hacia el SCBP (BPCS) únicamente debe ser unidireccional, ver detalle en puntos 8.6.4.1 y 8.6.6.4 de esta norma.

8.4.1.2 Sistema de gas y fuego (11.16 capítulo 5). Los sistemas de detección de gas y fuego y el SIS deben contemplar arquitecturas (sensores, procesador lógico y elementos finales) independientes, sin embargo, debe existir comunicación entre ellos. Estas requieren consideraciones de prueba automática, para permitir la detección de fallas del sistema en interiores; monitoreo en línea, técnicas de votación y diagnostico para asegurar que el sistema mantiene su disponibilidad para desempeñar su función. En algunos casos se requiere comunicación entre el sistema de gas y fuego y el SIS para reforzar la seguridad global. En el caso del sistema de gas y fuego la comunicación con el SIS es bidireccional en este la señal de gas y fuego a el SIS debe ser de acuerdo a las especificaciones de Pemex. (ver NRF-011 - SAAFAR).

8.4.2 Complejidad.

Los sistemas deben seleccionarse y diseñarse para minimizar la complejidad y que cumplan con esta norma, y el IEC 61508. Cada elemento del sistema debe especificarse bajo estándares de desempeño con la funcionalidad requerida, integridad de seguridad y estándares de desempeño y sobrevivencia, y no simplemente al más alto nivel alcanzable.

8.4.3 Concepto de falla segura.

El concepto de falla segura para plantas y equipo es el retorno al estado seguro en caso de falla del sistema lógico de protección, sensores, actuadores o fuentes de alimentación. Este requerimiento debe realizarse desenergizando para disparo las salidas del SIS (11.16 capítulo 4).

Durante la operación normal, con la planta en condiciones seguras, las entradas de los sensores de planta, el sistema lógico, y salidas a los dispositivos protectores estarán energizados. El sistema interpretará el estado desenergizado de una entrada como una demanda y se desenergizarán las salidas apropiadas para iniciar un paro. Este diseño debe asegurar también un paro por pérdida del suministro eléctrico a las entradas del sistema, salidas o lógica del sistema.
Se aplica el principio de falla segura para todos los equipos de la instalación. En este caso el contratista debe calcular el tiempo en que el sistema este en estado degradado sin comprometer la función de seguridad. En casos en donde no se aplique el concepto de falla segura por la naturaleza de la aplicación y sea necesario energizar para disparo (sistema de gas y fuego) se debe justificar y hacer consideraciones a fin de cumplir la integridad de seguridad requerida.

8.4.4 Tasas de falla y modos de falla (11.1 anexo B).

Las tasas de fallas reveladas y no reveladas y su implicación deben ser consideradas en el diseño del SIS. Al cuantificar la confiabilidad de un sistema se requiere de valores exactos de tasas de fallas de sus componentes. Desafortunadamente, frecuentemente no se cuenta con datos disponibles y si existen, no son confiables. Los datos son obtenidos a partir de registros específicos en bitácoras de la planta, fuentes genéricas y en base a opinión de expertos. La mejor opción es obtener las tasas de fallas a partir de registros específicos en bitácoras de operación y/o mantenimiento. Las fuentes genéricas son convenientes pero se debe tener precaución en su uso, particularmente porque la mayoría de ellas están basadas en la industria electrónica y nuclear. La opinión de expertos es una fuente accesible de datos y resulta efectiva si se analiza al sistema correctamente.

8.4.5 Integridad del sistema.

La integridad de los sistemas se refiere a la capacidad de dichos sistemas para operar bajo circunstancias dadas y esta relacionada con su confiabilidad y disponibilidad. Se expresa en términos del tiempo medio entre fallas (MTBF) o su recíproco, fallas por unidad de tiempo, independientemente de estos requisitos, al seleccionar y especificar un sistema se debe considerar además (11.16 capítulo 5):

a) Tasas de falla (reveladas y no reveladas).
b) Falla para actuar en demanda.
c) Tiempo medio de reparación real (MTTR).

Además, se deben emplear intervalos de prueba y tiempos de reparación en los análisis de confiabilidad y disponibilidad (no mayor a un año y no menor a tres meses) para el caso de instalaciones de Pemex.

Cuando no se disponga de información específica de los equipos o sistemas de interés, los análisis de confiabilidad y disponibilidad pueden basarse en análisis de tasas de falla de situaciones comparables o cálculos empleando métodos de pronóstico apropiados, como árboles de fallas o AMFE (FMEA) y aplicando información relevante como la contenida en la base de datos OREDA (11.13).

Fallas no reveladas en el sistema obstruirán su efectividad en seguridad. Deben tomarse acciones para eliminar estos modos de falla sobre el diseño o en su caso debe aplicarse un método de pruebas adecuado que permita revelar dichas fallas. El contratista debe garantizar las pruebas.

Para aplicaciones NIS 3 (SIL 3), un objetivo de diseño debe ser el evitar que una falla simple pueda ocasionar la falla de todo el sistema.

Para cada FIS (SIF) que requiera un NIS 3 (SIL 3) se debe hacer un análisis de confiabilidad y disponibilidad, y debe documentarse formalmente para garantizar que se cumpla la integridad de seguridad requerida. Se deben considerar los efectos de las fallas de causa común al calcular la integridad global del sistema.

Los sistemas lógicos deben estar especificados para la integridad o la función más alta de integridad que esté implantada.

Si Pemex considera conveniente, puede solicitar al contratista la certificación de los elementos que componen al sistema integrado de seguridad, como la de TUV, ya que a la fecha no hay compañías especializadas que certifiquen el SIS completo.

8.4.6 Redundancia.

Esta debe de aplicarse a fin de ampliar la integridad de seguridad o mejorar la tolerancia a fallas, el diseñador debe determinar los requerimientos de redundancia para lograr el NIS (SIL) y la confiabilidad requerida de todos los componentes del SIS como son sensores, procesadores lógicos y elementos finales de control. La redundancia se aplica tanto en los componentes físicos del sistema (hardware) como en los programas de cómputo (software).

8.4.7 Fallas de causa común.

Las fallas de causa común pueden ser provocadas por un componente único o por errores sistemáticos en los componentes redundantes. Las fallas de causa común y los errores sistemáticos deben ser reducidos por el contratista durante el proceso de diseño empleando medidas apropiadas de reducción de fallas. Entre las principales medidas de reducción que se deben considerar se tienen:

a) Proporcionar al proveedor información especifica del proceso (códigos, números de modelo, entre otros).
b) Verificación.
c) Separación diversa/ idéntica.
d) Redundancia diversa/idéntica.

En algunos casos sistemas diferentes pueden compartir el mismo ambiente, cabina, operador, interfase. Sin embargo dichos sistemas deben contar con fuentes de energía y procesadores lógicos separados físicamente para evitar fallas de causa común y a la vez permitir pruebas de mantenimiento o modificaciones, lo cuál debe considerarse durante el diseño del sistema.

8.4.8 Consideraciones de diseño de programas de cómputo (software).

En el diseño de un SIS deben considerarse los siguientes tipos de programas de cómputo (software):

a) Programas de cómputo integrados (software integrado).
b) Programas de cómputo de aplicación (software de aplicación).

8.4.8.1 Programas de cómputo integrados (software integrado). Este tipo de programas son parte del sistema proporcionado por el proveedor y no deben ser modificados por el usuario final.

El contratista debe proporcionar los programas de cómputo integrados (software integrado), los cuales deben ser transparentes para la preparación de programas de aplicación. Además debe proporcionar documentación que compruebe que:

a) Cuenta con un plan de calidad para los programas.
b) Está definida la versión de los programas integrados.
c) La versión de los programas integrados es la misma para la etapa de configuración, pruebas y puesta en operación.
d) Se revisaron y analizaron todas las ampliaciones o arreglos a la funcionalidad de los programas integrados contenidas en las nuevas versiones.

8.4.8.2 Programas de cómputo de aplicación (software de aplicación). Este tipo de programas contienen la lógica funcional del SIS en el sistema electrónico programable SEP (PES), en otras palabras, contiene las secuencias lógicas, permisivos, limites, expresiones, entre otros, que controlan las salidas, entradas, cálculos, y decisiones necesarias para alcanzar los requerimientos funcionales de seguridad. El prestador de servicios es el responsable de proporcionar el software de aplicación que cumpla con todas las especificaciones de seguridad del sistema.

En el desarrollo del software de aplicación se debe emplear el diseño modular y debe incluir módulos para pruebas de diagnostico.

Se debe emplear alguno de los siguientes lenguajes de programación certificados de acuerdo con la norma IEC-61131-3 (ver 10.8):

a) Diagramas de escalera.
b) Diagrama de bloques.
c) Listado de instrucciones.
d) Texto estructurado.

Deben establecerse patrones de programación para fortalecer un estilo consistente entre el equipo de diseño mediante la aplicación de un plan de calidad de los programas de cómputo. Para evitar complejidad innecesaria y características que dificulten el pronóstico del comportamiento del sistema, se deben considerar lo siguientes:

a) Los programas deben tener una estructura y un orden definido que garantice la comprensión de todo lo que ejecuta el programa en cualquier momento.
b) Cuando se apliquen secuencias anidadas, debe minimizarse el anidamiento.

Para verificar que el diseño de los programas de cómputo (software) de aplicación cumplen con cada uno de los requisitos establecidos en la especificación de requerimientos de seguridad, el prestador de servicios debe realizar:

a) Un análisis que demuestre que cada uno de los requerimientos de seguridad establecidos en la especificación se han implementado en el diseño.
b) Una revisión conjunta con Pemex de los diseños de las funciones críticas de seguridad.

Para confirmar que los programas de aplicación cumplen con los requisitos establecidos en la especificación de requerimientos de seguridad bajo todas las condiciones operativas esperadas, el prestador de servicios debe:

a) Desarrollar pruebas a los programas para someterlos a condiciones más allá de los límites normales de los datos, órdenes, entradas por teclado, y otras acciones.
b) Desarrollar un módulo de informe de errores y un módulo que permita resolverlos.

c) Desarrollar pruebas para los programas de aplicación que permitan determinar su comportamiento en presencia de fallas de los componentes físicos (hardware).
d) Presentar documentación que respalde cada uno de los puntos anteriores.

8.4.9 Agentes externos.

El sistema debe diseñarse de modo que el equipo tenga una inmunidad a disturbios electromagnéticos y a las inclemencias ambientales que impidan su funcionamiento adecuado. Las medidas tomadas deben verificar este requerimiento y serán seleccionadas de acuerdo a las consecuencias que se tendrían si el equipo fallara o presentara una degradación en sus funciones, además, el sistema no debe producir disturbios electromagnéticos que puedan interferir con la operación de otros equipos (11.16 capítulo 5).

El sistema debe diseñarse de tal forma que las funciones protectoras se mantengan bajo todas las condiciones climáticas posibles que existen en el lugar en que se instalará el sistema.

Las protecciones contra fuego, vientos y caída de objetos deben considerarse con relación a los estándares de desempeño. Estos deben tener en cuenta la sobre vivencia requerida y los modos de operación del sistema después de un accidente mayor.

8.4.10 Arquitectura.

La arquitectura del sistema indica el arreglo e interconexiones de los componentes o módulos del SIS. La selección de ésta es una actividad que debe desarrollarse durante el diseño conceptual del sistema. La arquitectura del SIS tiene un impacto directo en su integridad global de seguridad, influenciando asimismo en su confiabilidad. La selección de la arquitectura del SIS debe incluir las siguientes etapas (11.12 anexo B):

a) Selección de diseño energizado o desenergizado para disparo.
b) Selección de redundancia idéntica o diversa para los sensores, procesadores lógicos y elementos finales del control del SIS.
c) Selección de redundancia para las fuentes de potencia y de suministro de energía al SIS.
d) Selección de los componentes de la interfase con el operador.
e) Selección de las interfases de comunicación entre el SIS y otros subsistemas.

8.5 Verificación del Nivel de Integridad de Seguridad NIS (SIL).

La operación del sistema instrumentado de seguridad (SIS) se basa en un nivel de integridad de seguridad objetivo (NIS, SIL) que debe ser definido durante el desarrollo de la especificación de los requerimientos de seguridad (11.12 capítulo 5, ver punto 10.1 parte 2). La habilidad del SIS de lograr un NIS (SIL) específico debe ser validado en cada etapa de diseño y previo a cualquier cambio realizado al diseño después de la puesta en servicio. El contratista debe implantar un proceso de validación del NIS (SIL) para asegurar que el SIS cumple con la integridad requerida para cada función de seguridad, para entender la interacción de todas las funciones de seguridad y para entender el impacto de la falla de cada componente sobre el SIS.

El proceso de validación a implantar para la verificación del NIS (SIL) propuesto debe incluir los siguientes puntos:

a) Arquitectura y configuración de votación.
b) La instrumentación a utilizar.
c) Descripción del proceso.
d) Sistemas auxiliares o de apoyo (aire de instrumentos, agua de enfriamiento, central hidráulica, central eléctrica, entre otros) involucradas con las operaciones del SIS.

e) Frecuencia de prueba y definir si se realiza en línea o fuera de línea.
f) Procedimientos de prueba y equipo usados así como la probabilidad de que el equipo que integra el SIS comprometa su operación debido a las pruebas.
g) Modos de falla.
h) Tasas de falla.
i) Cobertura de diagnóstico.
j) Intervalos de reparación y si la reparación se realiza en línea o fuera de línea.
k) Procedimientos de mantenimiento y la probabilidad de que el SIS comprometa su operación debido a la reparación.
l) Procedimientos de administración de cambios, frecuencia de cambios, y la probabilidad de que se introduzca un error durante el cambio.
m) Disciplina de operación y mantenimiento, incluyendo una estimación de la frecuencia de error humano y circunstancias en las cuáles puedan ocurrir una maniobra incorrecta.
n) Procedimientos administrativos.
o) Fallas de causa común.
p) Fallas sistemáticas.
q) Identificación de las funciones de seguridad, sus entradas/salidas y sus dispositivos de campo.

La integridad de seguridad del SIS se mide en base a la probabilidad de falla en demanda (PFD), es decir, la probabilidad de que el sistema instrumentado de seguridad falle de tal manera que sea incapaz de realizar su función de seguridad asignada. La PFD se debe expresar como PFD_{prom}, el valor promedio sobre el intervalo de prueba funcional (11.24 parte 1, capítulo 4).

Para satisfacer los requerimientos de un NIS (SIL) dado, la PFD_{prom} debe ser menor que el límite superior en cualquier instante de tiempo durante el intervalo de prueba funcional. Para lograr esto, el SIS debe probarse manualmente, o bien, tener diagnósticos internos comprensivos.

Se debe seguir el siguiente procedimiento para la verificación del SIS (11.24 partes 2, 3 y 4):

a) Definir todos los posibles tipos de fallas del sistema: esto incluye fallas físicas y fallas sistemáticas, cada una de las cuáles a su vez se dividen en fallas independientes y fallas de causa común. Las fallas de causa común y fallas sistemáticas deben de ser evaluadas cuando un SIS implica un diseño complejo o inusual, cuando se trata de un sitio en donde existen antecedentes de falta de disciplina en operación y cuando existen cambios importantes en prácticas de administración que impacten a la operación del SIS y prácticas de mantenimiento.
b) Definir todos los posibles tipos de fallas de elementos del SIS: Dado que el objetivo de evaluar la integridad de seguridad es calcular la PFD_{prom} y el $MTTF^{falso}$, todas las fallas de los elementos del SIS se clasifican en fallas “seguras” y fallas “peligrosas”. Al mismo tiempo, se definen todas las fallas detectadas en línea mientras el SIS está operando (fallas detectadas) y aquéllas no detectadas en línea (fallas no reveladas). Las fallas de elementos finales (válvulas) se deben seleccionar para fallar en dirección segura dependiendo de su aplicación específica. Todas las fallas de suministro de energía se consideran que se encuentran en estado desenergizado. Esta clasificación de tasas de fallas se define en base al análisis de modos de falla, efectos y diagnóstico. Si no se conocen los modos de falla, se debe suponer que todas las fallas son peligrosas, si no se conoce la capacidad de cobertura de diagnóstico, se debe asumir que las fallas no son detectadas. Si no se conocen los factores Beta de causa común, un valor de 10% es el aplicable (11.24parte 2).
c) Determinar el factor de cobertura de diagnóstico (C) para cada elemento del sistema.
d) Modelación del sistema: La modelación de cualquier arquitectura de un SIS tolerante a fallas puede realizarse mediante el uso de análisis de árbol de fallas y modelos de Markov conforme al reporte técnico ISA-TR84.0.02 (11.24). El modelo de árbol de fallas se aplicará para sistemas simples o complejos que implican NIS (SIL) 1, NIS (SIL) 2 o NIS (SIL) 3, la representación gráfica de la lógica

de falla es fácil de entender por personal de diferentes disciplinas y existe una gran disponibilidad de herramientas de cómputo para facilitar los cálculos. En este caso, el contratista debe verificar y justificar todas y cada una de las suposiciones y restricciones hechas en dicho modelo. Para la verificación de SIS con NIS (SIL) 1, NIS (SIL) 2 y NIS (SIL) 3 se debe usar ISA-TR84.0.02-3 o equivalente. Los modelos de Markov se aplicarán para sistemas simples o complejos que impliquen NIS (SIL) 1, NIS (SIL) 2 y NIS (SIL) 3, ya que permiten modelar múltiples modos de falla de componentes diferentes, con estrategias de prueba o de reparación diferentes, capacidades de diagnóstico, de reparación y de prueba imperfectos o no ideales, causa común y secuencias de fallas dependientes del tiempo. Para la verificación de SIS con NIS (SIL) 1, NIS (SIL) 2 y NIS (SIL) 3 se debe usar ISA-TR84.0.02-4 o equivalente.

e) Para poder pronosticar la PFD_{prom} y el $MTTF^{falso}$ de un SIS se debe contar con datos de tasas de falla de los diferentes componentes del SIS. Existe una gran variedad de fuentes de datos de tasas de falla tales como bases de datos públicas, registros compilados de mantenimiento, datos de campo del vendedor, cálculos de confiabilidad (11.13) o experiencia operativa (11.12 anexo D). El contratista debe justificar la base de datos que use.
f) Usando la arquitectura del SIS fijada con anterioridad, calcular la $PFD_{promedio}$ para cada función de seguridad combinando las contribuciones de cada uno de los elementos del SIS que impacten a la función de seguridad en cuestión.
g) Determinar si la PFD_{prom} cumple las especificaciones de los requerimientos de integridad de seguridad para cada función de seguridad.
h) Si no se cumple con las especificaciones de los requerimientos de integridad de seguridad, se requiere modificar el SIS (configuración y/o selección de los componentes físicos o hardware, intervalo de prueba, incrementar la capacidad de diagnóstico, entre otros) y volver a calcular hasta cumplir con las especificaciones de los requerimientos de seguridad (11.24 parte 3).
i) Determinar la tasa de disparos en falso esperada para componentes del sistema y combinar para obtener $MTTF^{falso}$ para el SIS.
j) Si el $MTTF^{falso}$ calculado es inaceptable, se debe modificar la configuración (adicionar redundancia, usar componentes con mayor confiabilidad, entre otros) y recalcular hasta cumplir las especificaciones de los requerimientos de seguridad. Esto requerirá un recálculo de la $PFD_{promedio}$ para cada función instrumentada de seguridad.
k) Cuando los valores de $PFD_{promedio}$ y $MTTF^{falso}$ cumplen o exceden a los valores especificados en las especificaciones de los requerimientos de seguridad, el procedimiento de verificación ha terminado.

8.5.1 Documentación.

Una vez concluida la verificación del SIS el contratista debe presentar a Pemex la siguiente documentación en el formato aprobado previamente por Pemex:

a) Datos del SIS (compañía, planta, unidad, función de seguridad).
b) Consideraciones específicas para cada función de seguridad.
c) Referencia a los documentos de las especificaciones de los requerimientos de seguridad usados en el análisis.
d) Datos de tasas de falla.
e) Modelo: conjuntos de corte mínimo e índices de importancia en el caso de árboles de fallas y el modelo de Markov desarrollado en el caso de modelos de Markov.
f) $PFD_{prom.}$
g) $MTTF^{falso.}$
h) Estudios de sensibilidad y ¿Qué pasa si? (What if?). Un estudio de sensibilidad estima el cambio en la PFD_{prom} o $MTTF^{falso}$ para cálculos de incertidumbre en los datos de tasas de falla de componentes. Un estudio ¿Qué pasa si? (What if?), estima el cambio en la PFD_{prom} o $MTTF^{falso}$ con respecto a cambios en la configuración del SIS.
i) Recomendaciones y procedimientos detallados para mantenimiento y pruebas del SIS.

j) Detalles de cálculo: referencia del programa de cómputo usado si es que se usó alguno, así como las memorias de cálculo debidamente referenciadas conforme a la normatividad aplicable en cada una de sus etapas, para la transformación de los datos de tasa de falla de componentes en el formato de entrada al programa, opciones seleccionadas del programa de cómputo (software), archivos de entrada y salida (en disco o en forma electrónica) con su debida nomenclatura sobre la base de los DTI`s, ecuaciones empleadas, e interpretación de los resultados, entre otros.

8.6 Consideraciones del diseño detallado del SIS.

8.6.1 Interfases con el operador.

Las interfases con el operador sirven para comunicar información al operador tal como una acción de paro a tomar, diagnóstico del sistema, sensor, caja lógica, estado del elemento final, pérdida de energía que impacte la seguridad, entre otros. La operación del sistema sin embargo, no debe depender de la interfase, ya que no siempre puede estar funcionando o estar disponible.

La interfase del operador debe diseñarse usando principios de factor humano. La presentación de la información al operador debe ser clara y no ambigua. El volumen de alarmas y mensajes que se presentarán al operador en una situación delicada de la planta debe ser administrada y revisada.

El contratista debe asegurarse de no permitir botones configurados para desencadenar el paro de emergencia.

Los requerimientos se deben oficializar y deben registrarse basándose en el control de la información presentada en pantalla, para asegurar que se cumplan dichos requerimientos.

Los controles deben localizarse asegurando que sólo el personal autorizado podrá cambiar datos o acceder a los programas. El control de acceso se da mediante contraseña la cuál podrá ser cambiada cuando Pemex lo requiera y el contratista deberá de soportar lo pertinente para poder realizar dicho cambio.

En el diseño de la interfase de operación del SIS se deben considerar las fallas que puedan ocurrir en la interfase de operación con el SCBP (BPCS). En el diseño se debe tomar en cuenta las fallas de la interfase del operador del SIS, dando los medios como alternativas suficientes para que el operador lleve al proceso a un estado seguro y que las funciones automáticas del SIS no estén comprometidas. Pemex definirá en base a sus necesidades si la interfase del SIS será independiente de la del SCBP (BPCS) o si dicha interfase se integrara a la del SCBP (BPCS).

En el diseño del SIS se debe reducir al mínimo la necesidad de que el operador seleccione y desvíe el sistema mientras la unidad se está ejecutando. Si el diseño requiere el uso de acciones en operación, el plan incluirá los medios para proteger contra errores del operador.

El contratista debe proporcionar estación industrial para interfase humano maquina y equipo de cómputo de acuerdo a las especificaciones de la licitación.

Estado de la Información. La información del estado del SIS que es crítica para mantener el NIS (SIL) estará disponible en la interfase del operador. Esta información debe incluir:

a) Secuencia del proceso.
b) La indicación de que se ha activado la acción protectora del SIS.
c) La indicación de que una función de protección está desviada.
d) La indicación de que la(s) acción(es) es (son) automática(s) tal como la degradación del voteo del sistema y/o manejo de la falla ocurrida.

e) El estado de los sensores y los elementos finales del control.
f) La pérdida de energía y su localización, cuando ésta pérdida afecte a la seguridad.
g) Los resultados de diagnósticos de la comparación.
h) Fallas del equipo debido a las condiciones ambientales que afectan al SIS.
i) Histórico de alarmas y secuencia de eventos.
j) Pantallas operativas de mantenimiento periódico.
k) Registro para control y auditoria del mantenimiento del sistema.
l) Guías de operación para procedimientos críticos.

La interfase del operador debe usarse para comunicar información entre el SIS y el operador y debe Incluir los siguientes componentes.

a) Interfase humano – maquina para desplegados de pantalla.
b) Tableros que contengan lámparas, estaciones de botones, indicadores, e interruptores.
c) Anunciadores (alarmas audibles y visibles).
d) Impresoras.
e) Cualquier combinación de éstos.

La interfase humano – maquina para desplegados de pantalla. En caso de que Pemex lo requiera los desplegados de pantalla podrán ser compartidos por las funciones de control de proceso y de seguridad [un SCBP (BPCS), u otro sistema de control-básico] a través de los desplegados normales de operación.

Los desplegados relacionados con el SIS al operador deben actualizarse a la proporción requerida para comunicarse entre el operador y el SIS durante la condición de emergencia como una respuesta segura.

Los desplegados relacionados con el SIS deben identificarse claramente, evitando la ambigüedad o confusión potencial para el operador en una situación de emergencia. Los operadores deben tener fácil acceso a los desplegados relacionados con la seguridad, esto mediante un botón o por contacto directo en la pantalla que dará el acceso a una jerarquía del desplegado.

Se debe dar al operador información suficiente en un desplegado para que visualice rápidamente la información crítica. El desplegado debe ser coherente. Se deben proporcionar los mismos métodos de acceso, las alarmas convencionales, y el desplegado de los componentes usados en los sistemas no relacionados con la seguridad.

En el diseño del desplegado. Se deben emplear códigos de colores, indicadores brillantes, y datos importantes resaltados para guiar al operador a la información importante y reducir la posibilidad de confusión. Los mensajes deben estar claros y concisos.

Debe usarse la interfase del operador y un sistema asociado (como un sistema de control distribuido) para proporcionar automáticamente información relacionada con la seguridad, registrando en archivos históricos los eventos y funciones de alarmas. Las condiciones anotadas deben incluir los eventos del SIS (como el disparo y eventos previos al disparo).

Se debe desplegar una pantalla general de carácter dinámico que proporcione información en tiempo real del estado de la instalación y que permita la interacción con el sistema. Esta pantalla general debe desplegar un diagrama de la instalación que muestre de manera esquemática cada uno de los equipos, instrumentos (sensores, válvulas), cabezales y tuberías debidamente identificados mediante etiquetas o “tags” así como sus respectivas condiciones de operación. En la pantalla general se deben mostrar los diferentes instrumentos debidamente identificados y codificados mediante colores, que se muestran en la tabla 3, para indicación de su estado en tiempo real, así, si una válvula está abierta (usar color verde), si está cerrada (usar color rojo), en mantenimiento (usar color amarillo), prueba (usar color azul), manual (usar color magenta), estado de alarma presente (cambia de color entre rojo y verde). Además el programa debe permitir el acceso a detalle de cada

uno de los instrumentos de la instalación mediante el uso de desplegados de detalle (overlays), los cuáles deben proporcionar un icono con la representación esquemática del instrumento así como información particular en tiempo real de un instrumento determinado como es por ejemplo, la presión, sus unidades, en el caso de válvulas indicar si está abierta o cerrada, en prueba, mantenimiento, en modo manual, niveles de alarma y sus indicadores de alarma activa, así como botones para abrir otras ventanas como la de tendencia real, prueba parcial y mantenimiento.

La pantalla general debe mostrar un menú que permita desplegar a otras diferentes pantallas: a pantalla general, a pantalla de botones, lecturas de los sensores de todas las pantallas en unidades del Sistema Internacional (SI), una pantalla que muestre los sensores activados mediante iconos debidamente identificados, una pantalla de indicación de válvulas que se encuentren en mantenimiento mediante iconos debidamente identificados, una pantalla que muestre los diagnósticos del procesador lógico, una pantalla que permita acceder el login o contraseña del personal usuario, y una pantalla que muestre el estado de la UPS.

Color	Matiz	Saturación	Luminosidad	Tono Aproximado
Verde	90	240	100	
Rojo	0	240	110	
Amarillo	40	240	120	
Azul	160	240	120	
Magenta	200	240	120	

Tabla 3. Colores para indicación de estado en tiempo real.

En la pantalla de alarmas reales y en la pantalla de alarmas históricas se debe mostrar un desplegado que provea un sistema de notificación que informe al operador el estado del sistema y las condiciones del mismo. Este desplegado debe mostrar las variables que se encuentren en estado de alarma, además se debe desplegar las alarmas por prioridades y/o grupos de alarmas. El código de colores para los mensajes de alarmas históricas es el siguiente: Color rosa para alarma de eventos del sistema, color rojo para alarma activa sin reconocer, color amarillo para alarma activa reconocida, color azul para alarma no activa sin reconocer. En la pantalla de diagnóstico, al encontrar alguna falla se debe reflejar de manera coloreada en el diagrama de la tarjeta en la que se identificó la falla y se debe desplegar mediante un desplegado de detalle (overlay) otra pantalla que indique la falla posible.

Alarmas. Toda alarma será anunciada de manera sonora y visible de modo continuo hasta que sea reconocida por el operador. Los desplegados visuales deben ser intermitentes y de un color codificado para poder distinguir entre diferentes alarmas prioritarias. Deben usarse también diferentes tonos audibles para distinguir entre diferentes alarmas prioritarias. Las alarmas del SIS deben ser fácilmente visibles para el operador y deben ser reconocidas fácilmente con respecto a otras alarmas. El operador debe ser capaz de ver siempre que está pasando en el SIS aún cuando falle el SCBP (BPCS). Por tanto, las alarmas par el SCBP (BPCS) y para el SIS deben estar separadas físicamente para minimizar la posibilidad de que fallas de modo común en los subsistemas de alarmas afecten la operación tanto del SIS como del SCBP (BPCS).

Impresora(s). Las impresoras conectadas al SIS no deben comprometer la función de seguridad si la impresora falla.

Los SIS conectados a un SCBP (BPCS) deben utilizar recursos de éste para realizar sus funciones de registro relacionados con la seguridad y el informe de las funciones.

Las Impresoras deben documentar la secuencia de eventos, la información, los diagnósticos, y otros eventos relacionados con la seguridad y alarmas, registrados con tiempo en el cual ocurrió, fecha y número de identificación. La impresión de alarmas debe llevarse a cabo mediante una impresora dedicada exclusivamente para este propósito, no debe mandar a impresión una hoja por cada alarma y debe ser de manera continua. La impresora de reportes podrá compartirse con la de otro sistema.

8.6.2 Programas de cómputo (software) de aplicación del SIS.

El contratista debe proporcionar la especificación del software de aplicación apegándose a la especificación de requerimientos de seguridad del SIS establecidos por Pemex y a la arquitectura de los sub – sistemas.

Las entradas necesarias y las salidas generadas en cada una de las etapas del software de aplicación durante su Ciclo de vida, deberán cumplir lo indicado en la tabla 4.

Complementariamente el Contratista debe cumplir e incluir los siguientes elementos, si estos son parte del estándar de producto SEP (PES) y no son parte del software específico de aplicación:

a) Sistema operativo SEP (PES)
b) Sistema de manejo de telecomunicación SEP (PES)
c) Dispositivos de manejo del SEP (PES)

El software de aplicación debe cumplir los estándares de aseguramiento de calidad y debe satisfacer el nivel de integridad de seguridad requerido de la aplicación final. La evidencia de que se aplique el aseguramiento de calidad al desarrollo del software de aplicación debe ser parte del plan de calidad del software. El software de aplicación debe permitir cambios en línea sin inducir condiciones inseguras.

El plan de calidad del software de aplicación debe especificar o referenciar procedimientos para identificar fallas en el software de aplicación que son encontradas por otros usuarios y para incorporar cualquier corrección al software de aplicación.

Puede haber software de aplicación para los cuales se disponga de datos del buen desempeño en campo. Dichos sistemas pueden ser una alternativa adecuada para el desarrollo de software con altos estándares de aseguramiento de calidad. Sin embargo la importancia de tales datos de desempeño en campo debe evaluarse cuidadosamente. La evaluación debe confirmar que la evidencia de campo relaciona aplicaciones similares con la aplicación deseada, y que el software de aplicación no se modificó durante el período en el cual los datos de campo fueron empleados. La evidencia de campo no debe ser empleada para omitir evidencia de deficiencias de control en el diseño del software.

Los detalles de estándares de desempeño del software de aplicación que sean importantes para las especificaciones de los requerimientos totales deben identificarse en el plan de calidad de software. Tales requerimientos de desempeño deben incluir:

a) Restricciones de tiempo.
b) Integridad, rendimiento y retraso de mensajes de telecomunicaciones.
c) Los estándares de desempeño para degradación bajo condiciones de carga alta.

Existe la posibilidad de que versiones subsecuentes del software de aplicación no sean compatibles totalmente con elementos anteriores. La estrategia adoptada para asegurar el nivel de integridad de seguridad sobre actualizaciones del software de aplicación debe contemplarse en el plan de calidad.

El software de aplicación sujeto a actualizaciones de versión frecuentes puede incrementar su tamaño de modo que sea también necesario actualizar el hardware de soporte. Deben tomarse precauciones en caso de que el

soporte del proveedor esté disponible por un corto periodo de tiempo a partir de la última actualización de la versión del software.

Fase del Ciclo de Vida del Software		Alcance	Entradas	Salidas
Titulo	**Objetivos**			
Especificación de requerimientos de software de seguridad.	Especificar los requerimientos para el software en términos de los requerimientos de las funciones del software de seguridad y los requerimientos de integridad del software de seguridad. Especificar los requerimientos de las funciones del software de seguridad para cada sistema E/E/PE relacionado a la seguridad necesarios para implementar las funciones de seguridad requeridas. Especificar los requerimientos para la integridad del software de seguridad para cada sistema E/E/PE relacionado a la seguridad necesarios para alcanzar el SIL especificado para cada función de seguridad asignada a ese sistema E/E/PE relacionado a la seguridad.	Software de programación del SEP (PES)	Especificación de requerimientos de seguridad E/E/PES (IEC 61508-2).	Especificaciones de requerimientos del software de seguridad.
Planeación de la validación del software de seguridad.	Desarrollar un plan para validar el software de seguridad.	Software de programación del SEP (PES)	Especificaciones de requerimientos de seguridad del software.	Plan de validación de la seguridad del software.
Diseño y desarrollo del software.	**Arquitectura:** Crear una arquitectura del software de aplicación que cumpla con la especificación de los requerimientos de seguridad del software con respecto a los niveles de integridad de seguridad requeridos. Revisar y evaluar los requerimientos impuestos sobre el software por la arquitectura de los elementos físicos del sistema E/E/PE relacionado a la seguridad.	Software de programación del SEP (PES)	Especificaciones de requerimientos de seguridad del software. Diseño de la arquitectura de los elementos físicos del sistema E/E/PE relacionado a la seguridad.	Descripción de la arquitectura de diseño del software. Especificación de las pruebas de integración de la arquitectura del software. Especificación de las pruebas de integración del software electrónico programable.
Diseño y desarrollo del software	**Herramientas de soporte y lenguajes de programación**: Identificar un conjunto adecuado de herramientas, incluyendo lenguajes y compiladores, para el SIL requerido, sobre el ciclo de vida de seguridad completo del software que ayude a la verificación, validación, valoración y modificación.	Software Sistema SEP (PES) Herramientas de soporte; Lenguaje de programación	Especificaciones de requerimientos de seguridad del software; Descripción del diseño de la arquitectura del software.	Estándares de codificación y herramientas de desarrollo. Selección de herramientas de desarrollo.

Diseño y desarrollo del software de aplicación	**Diseño detallado y desarrollo (diseño del software del sistema):** Para diseñar e implementar software que cumpla con la especificación de requerimientos del software de seguridad respecto al nivel de integridad de seguridad requerido, el cual es analizable y verificable, y capaz de ser modificado de forma segura.	Componentes mayores y subsistemas del diseño de arquitectura del software	Descripción del diseño de la arquitectura del software; Herramientas de soporte y estándares de codificación.	Especificación de diseño del software del sistema; Especificación de pruebas de integración del software del sistema.
Diseño y desarrollo del software de aplicación	**Diseño detallado y desarrollo (diseño de módulos individuales de software):** Para diseñar e implementar software que cumpla con la especificación de requerimientos del software de seguridad respecto al nivel de integridad de seguridad requerido, el cual es analizable y verificable, y capaz de ser modificado de forma segura.	Diseño del Software Sistema	Especificación de diseño del software del sistema. Herramientas de soporte y estándares de codificación.	Especificación de diseño de módulos de software; Especificación de pruebas de módulos del software.
Diseño y desarrollo del software de aplicación	**Implementación detallada de código:** Para diseñar e implementar software que cumpla con la especificación de requerimientos del software de seguridad respecto al nivel de integridad de seguridad requerido, el cual es analizable y verificable, y capaz de ser modificado de forma segura.	Módulos individuales de software.	Especificación de diseño de módulos del software. Herramientas de soporte y estándares de codificación.	Listado de códigos fuente. Informe de revisión de códigos.
Diseño y desarrollo del software de aplicación	**Pruebas de módulos de software:** Para verificar que los requerimientos para la seguridad del software (en términos de las funciones de seguridad del software requeridas y la integridad de seguridad del software) han sido alcanzados –para demostrar que cada módulo del software desempeña su función especifica y no desempeña funciones no deseadas.	Módulos del software	Especificación de pruebas de módulos del software; Listado de código fuente. Informe de revisión de códigos.	Resultados de pruebas de módulos de software. Módulos de software verificados y probados.
Diseño y desarrollo del software de aplicación	**Pruebas de integración de pruebas:** Para verificar que los requerimientos para la seguridad del software (en términos de las funciones de seguridad del software requeridas y la integridad de seguridad del software) han sido alcanzados –para demostrar que todos los	Arquitectura del software	Especificación de pruebas de integración del software del sistema.	Resultados de pruebas de integración del software del sistema. Verificación y prueba del software del sistema.

	módulos, componentes y subsistemas del software interactúan correctamente para desempeñar su función especifica y no desempeña funciones no deseadas.			
Integración de electrónicos programables. (Elementos físicos y software)	Integrar el software a los elementos físicos , electrónicos programables objetivo.	Elementos físicos electrónicos programables; Software integrado	Especificaciones de las pruebas de integración de la arquitectura del software. Especificaciones de las pruebas de integración de electrónicos programables. Electrónicos programables integrados.	Resultados de las pruebas de integración de la arquitectura del software. Resultados de las pruebas de integración de electrónicos programables. Electrónicos programables integrados verificados y probados.
Procedimientos de operación y modificación del software	Proporcionar información y procedimientos acerca de las necesidades del software para asegurar que la seguridad funcional del sistema E/E/PE relacionado a la seguridad se mantiene durante la operación y la modificación.	Igual al anterior	Todo lo anterior, donde aplique	Procedimientos de operación y modificación del software.
Validación del software de seguridad.	Asegurar que el sistema integrado cumple con las especificaciones de los requerimientos del software de seguridad al Nivel de Integridad de Seguridad intentado.	Igual al anterior	Plan de validación de seguridad del software.	Resultados de validación del software de seguridad. Software validado.
Modificación del software	Hacer correcciones, mejoras o adaptaciones al software validado, asegurando que se mantiene el nivel de integridad requerido del software de seguridad.	Igual al anterior	Procedimientos de modificación del software; Peticiones de modificación de software.	Resultados del análisis de impacto de la modificación del software. Registro de modificación del software
Verificación del software	Hasta el punto requerido por el Nivel de Integridad de Seguridad, probar y evaluar las salidas de una fase dada del ciclo de vida de seguridad para asegurar exactitud y consistencia con respecto a las salidas y a los estándares proporcionados como entradas en esta fase.	Dependiente de la fase	Plan apropiado de verificación (depende de la fase)	Reporte apropiado de verificación (depende de la fase)
Evaluación de la seguridad funcional del software.	Investigar y llegar a un juicio sobre la seguridad funcional alcanzada por los sistemas E/E/PE relacionados a la seguridad.	Todas las fases anteriores	Plan de evaluación de la seguridad funcional del software.	Reporte de la evaluación de la seguridad funcional del software.

Tabla 4 . Ciclo de vida del software de aplicación: visión global.

8.6.3 Comunicación de datos.

Para efectos de esta norma se distinguen dos tipos de comunicación del SIS, interna y externa. La comunicación interna es aquella que se da al interior de los procesadores lógicos y está en función de la tecnología con la que fueron construidos, por lo que no se abunda más este aspecto en esta norma. En cuanto a la comunicación externa se debe considerar aquella que se lleva a cabo entre un SIS y uno o mas sistemas independientes para efectuar intercambio de información de monitoreo y de comandos de acción, el contratista debe verificar que esta comunicación no comprometa la integridad del SIS, por lo que el diseño de esta comunicación debe considerar los requerimientos para comunicación de datos de cada función de seguridad, de acuerdo con la norma IEC 61508-2 “Seguridad funcional de los sistemas eléctricos, electrónicos y/o de electrónica programable relacionados a la seguridad”, parte 2 “Requerimientos para sistemas eléctricos/electrónicos/electrónicos programables, relacionados con seguridad”:

8.6.4 Requerimientos de energía.

El diseño debe asegurar que cada fuente de energía cumpla las necesidades del SIS tal y como se determinó en las especificaciones de los requerimientos de seguridad. Las fuentes de energía incluyen a la energía eléctrica, energía neumática (aire de instrumentos) y energía hidráulica (central hidráulica) entre otros. La conexión a tierra se incluye dentro de la categoría de energía eléctrica (11.12 anexo B).

8.6.4.1 Fuentes de energía eléctrica. La fuente de energía eléctrica debe ser diseñada de modo que cumpla con los requerimientos de integridad de seguridad y de confiabilidad de la aplicación. La confiabilidad del SIS se debe incrementar mediante la adición de redundancia en la fuente de energía eléctrica, esto aplica para funciones del SIS que se energizan para disparo. Las unidades de suministro deben tener integrados fusibles de protección y protecciones por alto voltaje y alta temperatura. Las unidades deben incluir indicadores del estado de operación y alarmas en caso de que una unidad falle. Adicionalmente, en cada terminación de suministro de energía se debe contar con un fusible o debe estar protegido para prevenir que una falla en la conexión a tierra en una terminal afecte a los demás.

La redundancia en la fuente de energía eléctrica debe aplicarse mediante el uso de una fuente alterna con transferencia automática, un suministro de potencia ininterrumpible (UPS) o bien una batería de respaldo. Se debe contar con un interruptor de transferencia automática con reestablecimiento manual para la transferencia de la fuente de energía primaria a la fuente de respaldo en caso de pérdida del suministro de energía. Adicionalmente se debe contar con alarmas que indiquen al operador tanto la transferencia a la fuente secundaria de energía como la pérdida de la misma. El equipo de transferencia, incluidos los desconectadores de transferencia, deben funcionar de manera que todos los conductores de fase de una fuente de alimentación se desconecten antes de que se conecte cualquier conductor de fase de la segunda fuente.

Para la transferencia a fuentes alternas, los requerimientos mínimos a cumplir son (11.12 anexo B):

a) Detección de fallas previo a su impacto sobre la operación del SIS.
b) Transferencia a la fuente de respaldo sin impactar la operación del SIS.
c) Habilidad para mantener las UPS o baterías sin impactar la operación del SIS.
d) Minimizar fallas de causa común.
e) El tiempo de transferencia a la fuente alterna debe ser seleccionado de modo que se eviten picos. Así, para cargas críticas (con tiempo de interrupción permisible máximo de 4 milisegundos) la transferencia al suministro de respaldo debe realizarse mediante interruptores de estado sólido con tiempo de switcheo de cero. Mientras que para cargas semicríticas (con tiempo de interrupción permisible de 0.2-20 segundos) debe realizarse mediante interruptores electromecánicos.

Una lista de verificación de los puntos a considerar para energía eléctrica (corriente alterna) debe incluir (11.12 anexo B):

a) Rango de voltaje y corriente (incluyendo la sobrecorriente transitoria). NOM-001-SEDE-1999. (ver punto 5.3 parte B, apartado 220-10).
b) Rango de frecuencia nominal.
c) Armónicas.
d) Cargas no continuas (no lineales). Ver punto 5.3 parte B, apartado 220-10.
e) Tiempo de transferencia
f) Protección por sobrecarga y corto circuito. NOM-001-SEDE-1999. (ver punto 5.3 parte B, apartado 220-10).
g) Protección contra descargas atmosféricas (rayos).
h) Protección contra transitorios tales como picos, impulsos (ondas de sobrecorriente transitoria) y ruido eléctrico, entre otros.

Suministro de energía eléctrica para sistemas electrónicos programables y sistemas electrónicos. Los sistemas electrónicos programables y electrónicos tienen por lo general un rango de aislamiento de tensión de transición conductiva menor que para un sistema eléctrico, por tanto, se debe considerar protección adicional contra picos de corriente. Por esta razón, cuando se trata de sistemas electrónicos programables, se debe contar como mínimo con la capacidad de soportar picos sin dañar los componentes y sin errores de operación de acuerdo con NOM-001-SEDE-1999 (artículo 645) y se complementa con IEEE C37.90.1 “Pruebas para protección eléctrica de sobretensión” (ver puntos 5.3 y 11.8).

Como mínimo, el sistema estará en capacidad de soportar descargas electrostáticas de acuerdo con IEC 1000-4-2, nivel 3 (ver punto 10.7). Por lo tanto el sistema debe estar conectado a tierra de acuerdo a NOM-001-SEDE-1999.

Los sistemas electrónicos programables y los sistemas electrónicos deben incluir suministros internos de energía que convierten la(s) fuente(s) de energía eléctrica a menores niveles de voltaje para su uso. Se debe considerar la redundancia en el suministro de energía para cumplir con los requerimientos de confiabilidad de la aplicación (11.12 anexo B).

Los sistemas electrónicos programables y los sistemas electrónicos son más sensibles a ruido eléctrico (interferencia por radiofrecuencia, interferencia electromagnética entre otros), para estos casos, se debe aplicar blindaje, buenas prácticas en el cableado y una conexión a tierra apropiada (ver punto 8.6.4.2).

Las entradas/salidas (I/O) deben tener distribuciones separadas de energía y además deben estar protegidas por fusibles para minimizar causa común en el caso de una falla en el cableado. Debe existir una coordinación entre el sistema de fusibles para asegurar un impacto mínimo sobre la operación del sistema en caso de que un fusible se queme (se dispare).

Para mejorar la confiabilidad se deben usar UPS’s tipo rectificador de entrada o tipo redundante paralelo.

8.6.4.2 Conexión a tierra. Una lista de verificación de los puntos a considerar para la conexión a tierra debe incluir (11.12 anexo B):

a) Protección por corrosión. NOM-001-SEDE-1999 parte110-2.
b) Protección catódica.
c) Protección contra descargas atmosféricas (rayos). NOM-001-SEDE partes 250-86, 800-13, 820-10.
d) Protección de electricidad estática.
e) Blindaje de conexión a tierra. NOM-001-SEDE parte 310.
f) Conexión a tierra de punto simple. (5.1 parte 921-10).

g) Pruebas de conexión a tierra. NOM-001-SEDE-1999 partes 210-7(c), 250-45, 250-59 y 305-4(d).
h) Barreras de seguridad intrínseca de conexión a tierra. NOM-001-SEDE-1999 artículo 504.
i) Disponibilidad de terminales de conexión a tierra.

8.6.4.3 Fuentes de energía neumática. El aire de instrumentos debe ser filtrado, secado y continuamente monitoreado para asegurar que se mantenga una presión apropiada, además se debe contar con un sistema de respaldo para que se cumpla con los requerimientos de confiabilidad. El aire de instrumentos debe estar libre de partículas (polvo, mugre y sólidos) y de sustancias corrosivas, debe estar seco y libre de aceite. El sistema neumático debe cumplir con los requisitos mínimos de integridad de seguridad.

El punto de rocío a la salida del secador debe de estar al menos 281.15 K (8°C) debajo de la temperatura mínima ambiente local registrada. El punto de rocío no debe exceder 277.15 K (4°C) en la presión de la línea (11.2 capítulo 5).

El tamaño de partícula aceptable para el sistema de aire de instrumentos debe ser máximo 40 micrómetros. Para dispositivos especiales que requieran tamaños de partículas menores debe proporcionarse un sistema de filtración adicional para prevenir la entrada de polvos finos al sistema de distribución (5 micrómetros).

Cuando se detecte una baja presión en el sistema, deben existir señales de alarma, un sistema de respaldo, suministros de reserva o planes de contingencia (11.15 capítulo 4). Además, se deben tomar las consideraciones necesarias para iniciar un paro controlado en vez de permitir el disparo aleatorio de válvulas (11.2 y 11.3).

Se requieren compresores que no usen aceite en las partes expuestas al aire comprimido, deben ser capaces de operación continua y deben dimensionarse para un 200% del requerimiento del aire total de instrumentos (11.5).

Debe existir redundancia en el compresor energizado a partir de una fuente diferente de suministro de aire en el evento de que la fuente primaria falle. El compresor de reserva debe estar equipado para arrancar automáticamente cuando la presión de salida del secador caiga por debajo del valor deseado.

En caso de que la instalación no cuente con una fuente de aire de instrumentos Pemex indicara la fuente alterna.

8.6.4.4 Fuentes de energía hidráulica. La energía hidráulica se usa en donde no se encuentra disponible un servicio de energía neumática. El sistema hidráulico debe cumplir con los requisitos mínimos de integridad de seguridad.

El fluido hidráulico debe ser un aceite tipo hidráulico natural o sintético no inflamable para uso apropiado para alta presión, sistemas hidráulicos de alto desempeño y un rango de temperatura ambiente. El sistema hidráulico completo debe ser construido de acero inoxidable serie 300. El recipiente debe estar equipado con válvulas de venteo y de rompimiento de vacío a una presión no mayor de 13.7895 kPa (2 psig) positivos y 2.0684 kPa (0.3 psig) negativos. El recipiente debe contar con entradas y salidas adicionales para operaciones de llenado y de venteo. Se deben proporcionar filtros en los venteos para prevenir la contaminación. Cada unidad de energía hidráulica debe estar equipada con bombas y sistemas de transmisión redundantes. Las bombas deben ser de desplazamiento positivo y estar equipadas con válvulas de relevo internas. Los sistemas de transmisión deben ser dimensionados de modo que proporcionen el flujo de aceite hidráulico de diseño a la presión de relevo del aceite hidráulico. (11.6).

8.6.5 Control de cambios durante la etapa de diseño detallado.

La necesidad de cambios en el diseño debe evaluarse antes de la puesta en servicio del sistema considerando la base técnica para el cambio, el impacto en la seguridad debida al cambio, el impacto a futuro de dicho cambio en la operación y mantenimiento, así como el tiempo requerido para el mismo. Cualquier modificación debe realizarse siempre conservando las características de seguridad del diseño original (11.23 capítulo 13) ya que los cambios en el diseño pueden inadvertidamente eliminar consideraciones importantes de seguridad, o bien disminuir la efectividad de controles. Los cambios en el diseño del SIS deben estar bajo el control de una persona asignada como responsable. Deben existir sistemas de administración y procedimientos durante la fase de diseño del sistema para un control y monitoreo efectivo de los cambios. Los cambios deben ser verificados, probados y documentados antes de continuar a la siguiente etapa del ciclo de vida. Los cambios propuestos deben ser evaluados tanto por el personal de compañía responsable del diseño, como por personal de Pemex responsable del proyecto antes de la implantación de los mismos (11.16 capítulo 5).

8.6.6 Consideraciones de diseño de equipo de campo.

Los componentes localizados en planta de los sistemas de paro de emergencia deben ser identificados de acuerdo con los diagramas y la documentación, la identificación debe ser con etiquetas o rótulos permanentes donde estén localizados los equipos.

Cada dispositivo de campo debe contar con cableado propio al sistema de entrada y salida.

Los dispositivos de campo se deben seleccionar e instalar de tal forma que minimicen las fallas resultantes por condiciones ambientales y de proceso adversas Las condiciones adversas que deben considerarse son: corrosión, congelamiento dentro de las tuberías, sólidos suspendidos, polimerización, contaminación con carbón y temperatura y presión extrema.

8.6.6.1 Diversidad. La diversidad se emplea para evitar que ocurran fallas de causa común, ya que el empleo de la misma tecnología en los elementos físicos (hardware) o programas de cómputo (software) puede producir fallas de causa común. En aplicaciones SIS la diversidad se aplica en elementos redundantes, sólo si esta es necesaria para alcanzar los requerimientos de integridad de seguridad.

Debe evitarse el uso de componentes poco confiables al aplicar el concepto de diversidad.

En el diseño de un SIS se debe considerar la diversidad al momento de seleccionar elementos físicos (hardware), programas de cómputo (software) de aplicación y utilitarios.

En el caso de los elementos físicos para implementar diversidad se debe emplear:

a) Tecnología diferente.
b) Componentes de fabricantes o vendedores diferentes.
c) Productos diferentes del mismo fabricante.

En el caso de programas de cómputo (software) la diversidad debe considerar los siguientes puntos:

a) Programación de aplicaciones por diferentes programadores.
b) Empleo de algoritmos diferentes.
c) Empleo de tipos de datos, estructuras de datos y técnicas de almacenamiento de información diferentes.
d) Empleo de subrutinas de manejo de excepciones y/o errores diferentes.

e) En el caso de emplear librerías y subrutinas ya codificadas, se deben utilizar al menos dos librerías y subrutinas que realicen la misma función con diferente código.
f) Rutinas con cambio del orden de operaciones aritméticas en conversiones y operaciones.
g) Rutinas con cambio en la secuencia de operaciones entrada y salida de información (I/O).

8.6.6.2 Sensores. Los sensores del SIS deben estar separados del SCBP (BPCS), de lo contrario se puede ver comprometida la integridad del sistema de seguridad. Además los procedimientos de prueba, calibración y mantenimiento requeridos para sensores del SIS deben ser más estrictos que los procedimientos para los sensores usados en el SCBP (BPCS) y puede ser impractico o muy difícil realizar la prueba en línea de dispositivos de campo compartidos.

Los sensores inteligentes deben protegerse contra escritura a fin de evitar modificaciones, a menos que una revisión apropiada de seguridad permita el empleo de lectura/escritura y aprobada por Pemex

Se deben proporcionar metodologías de diagnóstico adecuadas (transmisores analógicos) para los sensores a fin de alcanzar el NIS (SIL) requerido.

Los sensores deben de estar conectados directamente al sistema lógico, no deben estar conectados a cualquier otro sistema que no sea parte del sistema instrumentado de seguridad.

Cuando se usen transmisores inteligentes, se deben establecer procedimientos que: aseguren el correcto uso del modo de salida forzada y que nunca se dejen en ese mismo modo de manera permanente, así como también se deben de establecer procedimientos para realizar cambios en la configuración/calibración de dichos transmisores.

Los requerimientos generales para operación a falla segura que se deben cumplir en sensores son:

a) Durante una operación normal de proceso los contactos de los sensores deben estar cerrados y energizados
b) En el caso de falla de energía, las señales de los transmisores deben ir a un estado seguro.
c) En el caso de usar transmisores, se deben configurar de tal forma que se pueda aprovechar la señal de fuera de rango que normalmente ofrecen los transmisores.
d) Cuando se requieran más de dos sensores, el contratista debe: Realizar conexiones separadas a proceso para cada sensor, las señales de entrada al procesador lógico las debe hacer en módulos de entrada separados o un módulo de entrada que garantice la reducción de fallas de causa común y cumpla con la integridad requerida.
e) En el caso de sensores del tipo interruptores, el contratista debe llevar a cabo los arreglos y cálculos necesarios para realizar la supervisión de los lazos correspondientes a estos sensores, la supervisión debe proveer la siguiente información: interruptor activado, interruptor desactivado, circuito abierto y corto circuito.

8.6.6.3 Válvulas. Las válvulas deben seleccionarse de acuerdo a las condiciones específicas del proceso y la función deseada. Por lo tanto, esta permitido el empleo de válvulas de bola, de mariposa, o algún otro tipo que justifique su uso en aplicaciones de seguridad, el contratista de asegurar que sean bridadas e instaladas de tal forma que cada brida de la válvula sea conectada a la contrabrida de tubería correspondiente, evitando así la presencia de espárragos que vayan de lado a lado de la válvula. Otros factores que deben considerarse para la determinación de los requerimientos de válvulas son: tiempo de cierre, tipo de cierre, o clase de fuga (la clase de fuga debe seleccionarse de acuerdo con el ANSI/FCI 70-2 (11.4) y el API-553 (11.6). Así, en estos estándares, para la clase II, la máxima fuga permitida es de 0.5% de la capacidad, para la clase III, la máxima fuga permitida es de 0.1% de la capacidad, para la clase IV es de 0.01% de la capacidad, para la clase V, se permiten 0.0005 ml por minuto de agua por pulgada de diámetro de orificio por lb/pulg^2 diferencial (5 x 10^{-12}m^3 por segundo de agua por milímetro de diámetro de orificio por bar diferencial), la clase VI no se debe exceder 6.75 ml por minuto y 45 burbujas por minuto para un diámetro nominal de 8 pulgadas. Se deben considerar también aspectos de sobrevivencia por fuego o resistencia al fuego [cumplir con API Spec 6FA (11.9), API 553 (11.6), API std 607 y

609 (11.7 y 11.8)]. En estos estándares, la máxima fuga en el asiento de la válvula no debe ser mayor a 400 ml/pulg/min (15.7 ml/mm/min) para un periodo de fuego de 30 minutos. La máxima fuga externa para un periodo de fuego de 30 minutos más el tiempo para enfriarse a 100°C (212°F) no debe ser mayor a 100 ml/pulg/min (3.9 ml/mm/min). La máxima fuga en el asiento de la válvula para una prueba a baja presión de duración de 5 minutos después de enfriar no debe ser mayor a 40 ml/pulg/min (1.6ml/mm/min). La máxima fuga externa para una prueba a baja presión de duración de 5 minutos después de enfriar (válvula en posición cerrada) no debe ser mayor a 20 ml/pulg/min (0.8 ml/mm/min). Con la válvula en posición abierta la fuga externa no debe ser mayor a 200 ml/pulg/min (8 ml/mm/min).

De acuerdo al API Spec 6D “Especificación para válvulas de tubería (Compuerta, bloqueo, bola y check)”, “Specification por pipeline valves (gate, plug, ball and check)” (punto 11.26), en las válvulas con sello no metal-metal no deben presentar fuyga visible alguna en la prueba de presión. Para válvulas con sello metal-metal, la tasa de fuga de la prueba de presión no debe exceder 0.15 ml/pulg del calibre nominal del miembro de cierre, tal como se especifica en la siguiente tabla (Tabla 5 de este documento). El miembro de cierre es aquélla parte de la válvula que se encuentra posicionada en la corriente de flujo, la cuál permite, obstruye o regula el flujo.

Diámetro Nominal	Tamaño de la válvula NPS	M/M	Máxima tasa de fuga (cm^3/mm/min)
50	2	51	0.31
80	3	76	0.46
100	4	102	0.61
150	6	152	0.91
200	8	203	1.21
250	10	254	1.52
300	12	305	1.83
350	14	356	2.14
400	16	406	2.44
450	18	457	2.74
500	20	508	3.05
550	22	559	3.35
600	24	610	3.66
650	26	660	3.96
700	28	711	4.27
750	30	762	4.57
900	36	914	5.48
110	42	1067	6.40
1200	48	1219	7.30
1400	54	1372	8.23
1500	60	1524	9.14

Tabla 5. Máximas tasas de fuga permisibles para pruebas de sellado hidrostático de alta presión. (Pruebas de sellado hidrostático metal-metal).

Otros factores a considerar son: Los requerimientos de corte, la experiencia que se tenga con las válvulas, modos de falla de la válvula, procedimientos operativos que disminuyan su efectividad, requerimientos de pruebas, requerimientos de diagnostico, requerimientos de indicadores de posición o interruptores de posición, entre otros. Estos factores junto con: la tasa de falla, el material del cual esta fabricada, entre otros deben ser claramente documentados.

Las válvulas deben llevarse a una posición segura en caso de falla de energía.

Cuando aplique y de acuerdo al diseño en particular de ciertas instalaciones es necesario contar con válvulas de desvío y de bloqueo, sobre todo en aquellas válvulas del SIS que cierran a falla de aire/energía y que de probarse en línea causen serios problemas operacionales, en otras ocasiones, es necesario proveer a la válvula del SIS sólo con bloqueos (por ejemplo en válvulas que a falla abren). En los casos donde se requiera contar con desvío y bloqueos, se debe considerar la instalación de dos válvulas de purga/venteo (dependiendo del servicio en la línea) instaladas entre las válvulas de bloqueo corriente arriba y corriente abajo de la válvula del SIS, en este caso, se deben utilizar interruptores de posición que alarmen en el cuarto de control del SIS cuando la válvula de desvío sea abierta o cuando alguna de las válvulas de bloqueo sean cerradas. Las válvulas de desvío (by pass) y de bloqueo deben ser mecánicamente enclavadas a fin de evitar que las válvulas de corte del SIS puedan ser desviadas o bloqueadas respectivamente de forma inadvertida.

Las válvulas deben dimensionarse de acuerdo al IEC 60534-2 (ver 10.5). Todas las válvulas deben de contar con indicadores de posición local. Se debe rotular con flechas en ambos lados de la válvula la dirección del flujo.

Cuando se requieran más de dos válvulas, el contratista debe: Realizar conexiones a proceso y eléctricas separadas e independientes para cada válvula (ya sea que se requieran dos válvulas para el SIS o una para el SIS y otra para el SCBP), las señales de salida del procesador lógico las debe hacer en módulos de salida separados o un modulo de salida que garantice la reducción de fallas de causa común.

Actuadores. El actuador debe contar con un indicador local que muestre la posición de la válvula. En caso de pérdida de señal o suministro de aire la válvula debe tomar una posición segura y emitir una señal de alarma.

Dependiendo de la evaluación del nivel de integridad NIS (SIL) se determina el empleo de actuadores sencillos de retorno por resorte operados neumática o hidráulicamente, hidráulicos, neumáticos o actuadores de doble acción.

En caso de requerirse actuadores hidráulicos, el acumulador debe ser de tipo pistón con indicador de posición, deben existir tanques de suministro de respaldo neumático cargados con nitrógeno instalados cerca de la válvula.

Se deben tomar las medidas preventivas apropiadas para evitar que las líneas de descarga del actuador de la válvula se aíslen lo cual provocaría que la válvula no realice su función.

Se debe especificar un transmisor de posición. Se deben emplear actuadores neumáticos de tipo diafragma o pistón.

A menos que este justificado por las condiciones de operación se podrán emplear actuadores hidráulicos o eléctricos.

En caso de pérdida de señal la válvula debe tomar una posición segura.

Se deben emplear posicionadores electroneumáticos para control remoto.

La localización de la válvula de corte con respecto a la válvula de control dependerá de la posición de dicha válvula de control, si se encuentra a la entrada de un sistema, la válvula de corte debe estar localizada corriente abajo de la válvula de control, en caso de que la válvula de control se encuentre a la salida de un sistema, la válvula de corte debe localizarse corriente arriba de la válvula de control.

Materiales. El contratista debe de garantizar que los materiales suministrados cumplan con lo especificado en el diseño en cuanto a resistencia al medio de proceso, las condiciones de operación, el tiempo de vida y el estrés mecánico que acompaña a la operación requerida y en caso de que el diseño lo requiera se debe cumplir con los requerimientos de sobrevivencia.

Diagnóstico. Se debe introducir cobertura de diagnóstico para cumplir con el criterio de confiabilidad y con el propósito de incrementar los intervalos de prueba. El diagnóstico asociado a válvulas debe considerar dos condiciones establecidas: operación normal y diagnóstico activo.

El diagnóstico de la válvula durante operación normal debe considerar pruebas en línea, el uso de alarmas en caso de que la válvula cambie de estado sin una señal lógica, entre otros.

Para el diagnóstico activo de la válvula se deben instalar transmisores de posición o interruptores de límite para retroalimentar al sistema lógico indicando si la válvula operó correcta o incorrectamente, además se debe llevar a cabo considerando la secuencia del paro de emergencia.

Panel de control. Para funciones de seguridad críticas en caso de requerirse un panel de control local de válvulas, el acceso a éste, debe restringirse a fin de evitar el accionamiento inadvertido o no autorizado de las válvulas.

Válvulas solenoides. Se deben considerar la implantación de válvulas solenoides redundantes para aplicaciones críticas de seguridad en caso de que el diseño lo requiera.

No se deben usar para aplicaciones de SIS válvulas solenoides con mecanismos manuales que pueden ser operados cuando la bobina es des-energizada.

Las válvulas solenoides deben ser capaces de soportar altas temperaturas incluyendo el calor generado por si misma, la radiación proveniente de hornos, entre otros.

Debido a que una de las fallas más comunes en solenoides es cuando se queman las bobinas causando un disparo, deben usarse bobinas dobles para mantener al solenoide energizado si una de las bobinas se quema.

Las válvulas solenoides pueden emplearse en líneas de señales o pulsos con aire, hidráulicos o algún otro de acuerdo a las condiciones de la instalación y de conformidad con Pemex.

Las posiciones de montaje de válvulas solenoides deben elegirse de modo que aseguren la operación a falla segura de la válvula. Si la válvula tiene un posicionador, el solenoide debe ser instalado para ventear al actuador y no al posicionador.

8.6.6.4 Procesador lógico (10.6, parte 3)**.** El procesador lógico debe estar diseñado a falla segura en caso de pérdida de energía o bien cuando falla el sistema o alguno de sus componentes clave.

El procesador lógico y sus módulos deben contar con autodiagnóstico. La lógica interna de cada CPU debe traer incorporadas rutinas diagnósticas y de prueba automática en línea, y detección de fallas para determinar el estado de cada módulo o del subconjunto que está dentro del sistema. La unidad de control debe ser capaz de funcionar de acuerdo a los parámetros climáticos propios del sitio de instalación, ser resistente a los golpes, vibración, descargas electrostáticas, “surge” eléctrico e interferencia electromagnética y radiofrecuencia.

El procesador lógico debe cumplir por si solo íntegramente con la IEC-61508 (ver 10.1), contar con aprobación certificada bajo IEC-61508 para aplicaciones en el nivel de integridad requerido, toda la configuración debe estar basada en la IEC-61131 (ver 10.6 parte 3), en versiones Windows NT o versiones más actualizadas, con características de seguridad tales como clave de acceso administrativo, para operación y control de accesos. Además, el contratista debe asegurar que cumplirá con todas y cada de las restricciones que la certificadora imponga.

A la unidad de control se le debe dar mantenimiento en línea sin perder la protección. Los diagnósticos en línea estarán en capacidad de identificar, localizar y reportar las siguientes fallas:

a) Fallas permanentes en las cuáles un componente del sistema o algún módulo sufre una falla irreversible.
b) Fallas temporales al azar en los cuáles los defectos sucesivos están interrelacionados.
c) Fallas intermitentes donde aparecen funcionamientos defectuosos con algún grado de periodicidad.
d) Fallas de circuitos de detección de escrutinios y fallas.
e) Fallas de memoria, todas las funciones RAM y ROM.
f) Fallas de microprocesador.
g) Fallas de comunicación.
h) Interfase de entrada y salida y fallas de direccionamiento.
i) Fallas de módulo de entrada y salida.
j) Fallas de suministro de energía.
k) Problemas de sensor de campo (donde aplique).
l) Circuitos de I/O (entradas/salidas) abiertos o en corto circuito.
m) Alambres interrumpidos, bobinas de relé, contactos, terminales y fusibles de I/O abiertos.

El proveedor debe dimensionar el procesador lógico de acuerdo a lo solicitado por Pemex y el NIS (SIL) correspondiente. El proveedor debe suministrar los manuales de instalación, programación, operación y mantenimiento del equipo propuesto.

La unidad de control programable debe contar con un elemento de memoria, con capacidad de almacenamiento de datos de por lo menos 2 MB (mega bites) de memoria SRAM para la captura de secuencia de eventos, la cuál debe mantenerse íntegra aún en el caso de falla de energía; la memoria del programa debe ser del tipo no volátil o respaldada por batería. Se deben suministrar los medios para tener acceso local a la información contenida en este elemento de memoria y direccionar esta base de datos de eventos a un nivel superior de un sistema informático, si éste existe, a indicación de Pemex, bajo las características de compatibilidad total (protocolo de comunicación, interfase humano-máquina y demás características del sistema informático).

El procesador debe contar con los módulos de entrada/salida necesarios para recibir y transmitir las señales analógicas y discretas de/hacia los dispositivos de campo, que conformen el sistema.

Los módulos de entrada/salida no deben tener ningún punto singular de falla en modo común que pueda afectar más de un canal.

Se podrá aplicar cualquier tecnología para desvíos de entradas debiendo el contratista soportar sus procedimientos de acuerdo a los lineamientos de TUV.

En caso de falla de un canal o módulo de entrada/salida del dispositivo, se debe tener la capacidad de detectar la falla y mostrarla alarmando por algún medio.

Los módulos de entrada/salida averiados, deben detectarse en el procesador lógico por un diodo emisor de luz en el frente del módulo en falla.

Los módulos de entrada/salida deben contar con los siguientes diagnósticos y protecciones por canal: diagnóstico y protección de corto circuito y/o sobrecorriente y diagnóstico de circuito abierto.

Todos los módulos de entrada/salida del procesador deben poder ser reemplazados en línea sin interrumpir la energía eléctrica y sin requerir herramientas especiales; el reemplazo comprenderá la configuración automática sin que cause interrupción o disturbios en el monitoreo, lógica y actuación del sistema.

En el caso de requerirse, los contactos de salida del sistema lógico deben estar normalmente cerrados.

Es responsabilidad del contratista proporcionar datos de MTTF del procesador lógico, tasa de fallas del revolvedor lógico, el listado de los modos de fallas no reveladas y la frecuencia con que ocurren fallas identificadas, así como especificar el método utilizado y la fuente de dichos datos.

8.6.6.5 Cableado y líneas de control. Se debe considerar desde la etapa de diseño la protección a los cables y líneas de control asociadas al sistema instrumentado de seguridad (SIS), se debe dar protección con recubrimiento de vinilo por ataque de grasas y solventes así como realizar la ruta de cables a través de conduit para protección mecánica.

Por ningún motivo, se deben compartir los conduit para albergar cables de control de proceso, del sistema instrumentado de seguridad y de cualquier otro sistema eléctrico El tubo (conduit) no-metálico se debe instalar como un sistema completo, como establece el artículo 300 de la NOM-001-SEDE, y se debe sujetar firmemente a menos de 1 m de cada caja de salida, de unión, de conexiones, de cada gabinete o accesorio. El tubo (conduit) se debe sujetar como mínimo cada 1 m. El número de conductores en tubo (conduit) no debe superar lo permitido en la tabla 10-1 del capítulo 10 de la NOM-001-SEDE, según el tamaño nominal del tubo (conduit) que aparece en la tabla 10-4 del capítulo 10 de la NOM-001-SEDE.

Se debe evitar tanto como sea posible que las rutas de cables pasen por áreas de alto riesgo o muy vulnerables. En casos inevitables se requiere previa autorización de Pemex.

Otro rubro importante que se debe considerar es la de proteger al sistema de interferencia electromagnética, es decir, aquellos cables que lo requieran, se deben especificar con blindaje.

8.6.6.6 Protección por fuego, onda expansiva, caída de objetos u otros. Cuando se haya especificado algún requerimiento de sobrevivencia, la instrumentación y componentes involucrados tales como, actuadores, cables y cualquier otro dispositivo que formen parte del sistema instrumentado de seguridad deben especificarse con las respectivas protecciones por fuego, onda de choque, fenómenos meteorológicos y por caída de objetos sobre ellos.

8.6.6.7 Consideraciones ambientales. En la selección de los dispositivos que conforman el sistema instrumentado de seguridad se deben fijar los requerimientos concernientes a calor, escarcha por heladas, protecciones por ingreso de agua contraincendio (agua tratada, de mar, cruda, etc.) y/o por ingreso de otros medios de extinción de fuego.

Los dispositivos eléctricos deben especificarse de acuerdo con la clasificación de áreas peligrosas y deben ser consistentes con la filosofía o lineamientos de seguridad de la instalación.

8.6.6.8 Personal responsable y competente. En caso de que la operación y/o mantenimiento de la instalación se realice por un contratista, el personal responsable deberá cumplir con los siguientes puntos:

8.6.6.8.1 Personal responsable. Cada sistema de protección debe estar bajo el control de una persona identificada e informada de las responsabilidades asignadas a él. La persona asignada es responsable de asegurar que el sistema se mantenga ejecutando sus requerimientos de desempeño. Algunas (pero no limitadas) responsabilidades específicas son:

a) Asegurar que los operarios, el grupo de mantenimiento y personal técnico quienes trabajan con o en el sistema instrumentado de seguridad tengan la competencia necesaria para ello.
b) Controlar el acceso al sistema incluyendo el uso de llaves y contraseñas.
c) Coordinar las pruebas del sistema.

d) Controlar los cambios al sistema.
e) Asegurar que los registros más importantes sean mantenidos.
f) Evaluar los resultados de pruebas, de actividades de mantenimiento, fallas del sistema y tasas de demanda del sistema para asegurar que la integridad se conserva.

8.6.6.8.2 Personal competente. Todas las actividades del ciclo de vida del sistema instrumentado de seguridad deben manejarse y ejecutarse por personal competente, se listan algunos de los requerimientos que se deben considerar:

a) Tener conocimientos de ingeniería, entrenamiento y experiencia en: la aplicación del SIS al proceso, la tecnología usada, sensores, procesador lógico y elementos finales.
b) Contar con conocimiento de seguridad de procesos (análisis de seguridad del proceso).
c) Contar con las habilidades y conocimientos adecuados para desempeñar sus labores en el ciclo de vida del sistema instrumentado de seguridad.
d) Entender las consecuencias de potenciales de eventos indeseables (fallas en demanda, disparos en falso, entre otros).
e) Entender significado e implicación de los distintos niveles de integridad de seguridad NIS (SIL) de las funciones instrumentadas de seguridad FIS (SIF).
f) Entender las novedades y complejidad de la tecnología aplicada al sistema instrumentado de seguridad (SIS).

8.7 Pruebas de aceptación de fábrica, PAF (FAT).

El sistema debe ser completamente probado antes de ser enviado por el proveedor al usuario final (Pemex).

Todos los individuos involucrados con la construcción y la verificación del sistema bajo prueba deben participar en las pruebas PAF (FAT). Estas pruebas deben ser completadas en el sitio de fabricación previo al envío al usuario final, debe probarse tanto el hardware como el software que se está suministrando.

El sistema debe ser revisado y probado en un ambiente controlado, de manera que cualquier problema pueda ser resuelto y corregido usando los recursos disponibles en el sitio del proveedor. Las pruebas PAF (FAT) deben incrementar el entendimiento del personal de diseño y deben aclarar y rectificar cualquier duda.

El número de participantes depende de la complejidad y del tamaño del sistema. Se deben definir las responsabilidades de cada individuo participante de la PAF (FAT). Debe participar el siguiente personal:

a) Representantes del contratista (pueden participar: los proveedores de cada uno de los diferentes subsistemas e integrador del sistema). El contratista es el responsable de conducir y coordinar las pruebas PAF (FAT), así como de preparar los procedimientos de prueba requeridos.
b) Representante de Pemex.

El contratista debe probar el hardware del sistema lógico completo incluyendo los módulos de entrada/salida, las terminales, el cableado interno, los procesadores, los módulos de comunicación y la interfase del operador, el software (de operación y de aplicación), así como la redundancia.

Las pruebas deben basarse en un procedimiento documentado el cual debe ser proporcionado por el contratista y aprobado por Pemex. Las pruebas deben realizarse usando los siguientes criterios:

a) Inspección visual.
b) Suministrando entradas, usualmente digitales, pulsos, 4-20 mA, o T/C y observando la respuesta del sistema.

c) Manejando salidas, usualmente digitales o de 4-20 mA.
d) Creando varios escenarios de falla para probar los sistemas de respaldo.
e) Pruebas de la lógica no interactiva, esto es, la lógica que no requiere una retroalimentación de los dispositivos de campo para operar.
f) Simulación lógica para una prueba completa de la lógica. Esto es, probar funcionalmente el sistema electrónico programable y la interfase del operador sin que las entradas/salidas de campo se encuentren conectadas. La prueba debe realizarse antes de la instalación en campo fuera del ambiente de la planta. En la simulación, debe usarse la misma interfase del operador que va a ser usada en el sitio. Los sistemas electrónicos programables deben probarse mediante la técnica comúnmente conocida como “emulación dentro del procesador”.
g) El sistema se debe probar al 100%.

La simulación lógica debe hacerse de manera escrita en el procesador, las salidas son ligadas a las entradas dentro de la simulación, de modo que cuando una salida es enviada desde el sistema lógico, debe obtenerse una confirmación de que el dispositivo de salida ha operado. De este modo, la lógica es interactiva con los dispositivos de campo. La complejidad y exactitud de la simulación dependerá de la cantidad de tiempo, esfuerzo y recursos empleados. Esto dependerá de los requerimientos y expectativas de Pemex. El programa de simulación debe ser completamente separado de la lógica principal. La lógica de simulación debe ser removida completamente antes de las pruebas de aceptación y prearranque. Personal experimentado y entrenado por parte del contratista el cual debe escribir los paquetes de simulación. Se debe utilizar la interfase del operador como la interfase para la prueba lógica y para entrenamiento.

Si durante las pruebas PAF (FAT) se detecta la necesidad de una o más modificaciones, el contratista debe efectuar un análisis de impacto sobre la integridad del SIS.

Todos los equipos usados para la calibración y pruebas deben presentar certificados de calibración por parte del contratista.

8.8 Instalación, comisionamiento, operación, mantenimiento y pruebas.

El embalaje y transportación del equipo es responsabilidad del contratista quien debe garantizar la integridad de los equipos que conforman el SIS.

8.8.1 Instalación del SIS y comisionamiento.

En esta etapa se debe asegurar que el sistema instrumentado de seguridad sea instalado de acuerdo con el diseño detallado y la especificación de los requerimientos de seguridad. Durante la instalación y comisionamiento el contratista debe proporcionar lo siguiente:

a) Las actividades de instalación y comisionamiento.
b) Los procedimientos, medidas y técnicas a usar para la instalación y comisionamiento.
c) Programa de dichas actividades y tiempos.
d) Las personas, secciones y organismos responsables para estas actividades.

NOTA: La planeación de la instalación y comisionamiento deben integrarse en el proyecto global apropiadamente. Todos los componentes del SIS se deben instalar apropiadamente en base al diseño y el plan de instalación.

Como requerimientos generales asociados al proceso de instalación se tienen:

a) El contratista debe considerar la instalación del SIS de manera separada con respecto al trabajo eléctrico y electrónico de otros sistemas.

b) El contratista debe asegurarse que el paquete de diseño esté completo.
c) Todos los dispositivos montados en campo deben ser instalados de modo que permitan fácil acceso tanto para el mantenimiento como para las pruebas en línea que puedan ser llevadas a cabo.
d) El contratista no debe realizar ningún cambio a la calibración de los dispositivos de campo existentes.
e) Se debe proteger a todos los dispositivos de campo de daño físico o ambiental previo a la instalación.
f) El contratista no debe realizar ningún cambio o desviación de los diagramas de diseño sin previa autorización de Pemex en forma escrita y debidamente registrada.

Comisionamiento. El comisionamiento constituye una verificación física que confirme que el equipo, los dispositivos de campo y el cableado se encuentren físicamente instalados de acuerdo al diseño y listos para las pruebas PAS (OSAT). Dicho comisionamiento debe ser realizado por el contratista bajo supervisión de Pemex.

8.8.1.1 Pruebas PAS (OSAT) del SIS. Una vez que se ha completado el comisionamiento, el contratista debe realizar las pruebas PAS (OSAT) del SIS y someterlas a aprobación de Pemex. Dichas pruebas consisten en una verificación operacional de cada una de las funciones instrumentadas de seguridad (FIS), mediante la introducción de señales simuladas desde campo para verificar la correcta operación de los dispositivos de campo y de las entradas/salidas del sistema lógico después de que el sistema es energizado.

El contratista debe presentar lo siguiente antes de iniciar las pruebas PAS (OSAT):

a) El acta de aceptación de las pruebas de aceptación en fabrica PAF (FAT).
b) El protocolo de las pruebas de aceptación en sitio PAS (OSAT) aprobado por Pemex, el cual debe contener: las actividades a realizar, responsables, cómo se van realizar, criterios de aceptación, formatos de registros.

En esta fase el contratista debe confirmar lo siguiente:

a) Que las fuentes de energía son operacionales.
b) Que todos los instrumentos han sido calibrados de acuerdo a los requerimientos de operación.
c) Que todos los dispositivos de campo, el procesador lógico y sus entradas/salidas son operacionales.

8.8.1.2 Pruebas integrales del SIS. En caso de que el SIS forme parte de un proyecto integral en el cuál existan otros equipos que tengan interrelación con el SIS, el contratista debe realizar pruebas integrales del sistema que confirmen la funcionalidad correcta del sistema completo, incluyendo la lógica de acuerdo a las especificaciones de los requerimientos de diseño. Esta verificación debe realizarse después de que las pruebas PAS (OSAT) han sido completadas de manera satisfactoria.

El contratista debe presentar lo siguiente antes de iniciar las pruebas integrales:

a) El acta de aceptación de las pruebas PAS (OSAT).
b) El protocolo de las pruebas integrales aprobado por Pemex, el cual debe contener: las actividades a realizar, responsables, cómo se van realizar, criterios de aceptación, formatos de registros.

Durante las pruebas integrales del SIS el contratista debe incluir la confirmación de los siguientes puntos:

a) Que el SIS se comunique (cuando sea requerido) con el Sistema de Control Básico de Proceso o cualquier otro sistema o red.

b) Que los sensores, el procesador lógico, y los elementos finales se desempeñen de acuerdo con lo especificado en los requerimientos de diseño.
c) Que los dispositivos de seguridad operen correctamente al punto de ajuste (setpoint) definido en la especificación de los requerimientos de diseño.
d) Que la secuencia de paro sea la correcta.
e) Que el SIS proporcione indicaciones visuales de que se encuentra funcionando correctamente.
f) Que las funciones de restablecimiento total y parcial del sistema se encuentren acordes a como se planeó.
g) Que las funciones de bypass y de restablecimiento de bypass operen correctamente.
h) Que los sistemas de disparo manual operen correctamente.
i) Que la documentación del SIS sea consistente con la instalación final y con los procedimientos de operación.
j) Que el SIS actúe bajo los modos de operación normal y anormal como está definido en la especificación de diseño.
k) Confirmar que el desempeño inadecuado del SCBP (BPCS) y otros sistemas conectados no afecten el funcionamiento del SIS.
l) Verificar que las comunicaciones entre el SIS y el SCBP (BPCS) o algún otro sistema no afecten la integridad y funcionalidad del SIS.
m) Las funciones de alarma y diagnóstico operan como se requiere.
n) Confirmar que el SIS opera como se requiere cuando se presenta el evento de pérdida de energía o falla de algún suministro de energía y que retorna al estado deseado una vez que la energía es restaurada y la función de restablecimiento haya sido activada.

Todos los equipos usados para la calibración y pruebas deben presentar certificados de calibración por parte del contratista.

La documentación requerida para soportar las pruebas integrales depende de la complejidad del sistema de seguridad y de los documentos que fueron originalmente preparados durante el diseño. La documentación de las pruebas integrales del SIS debe incluir los siguientes puntos:

a) Procedimientos de la verificación completa de las pruebas integrales.
b) Copia de la especificación de los requerimientos de diseño.
c) Listado impreso del programa del procesador lógico.
d) Un diagrama de bloques del sistema global.
e) Una lista completa de las entradas/salidas.
f) Diagramas de proceso e instrumentación.
g) Índice de instrumentos.
h) Diagramas de lazos.
i) Esquemas eléctricos.
j) Matriz de Paro de Emergencia.
k) Planos que indiquen la localización de los equipos principales (PLG).
l) Diagramas de conexiones en gabinetes, diagramas que indiquen la interconexión y las terminales de todos los cables.
m) Diagramas de tubings del sistema neumático.
n) Documentación del proveedor del equipo, incluyendo especificaciones, requerimientos de instalación, y manuales de operación.
o) La fecha en que se realizó la prueba integral.
p) Referencia a los procedimientos usados en la prueba integral.

q) Constancia de aceptación por parte de Pemex de que el contratista ha completado de manera satisfactoria la prueba integral.

Si se presenta el caso que durante la prueba integral no se cumple con los requerimientos establecidos durante el diseño, la diferencia debe ser evaluada por el contratista y debe informar a Pemex las implicaciones sobre la integridad del sistema que ocasiona esta diferencia y si es necesario regresar a alguna etapa anterior en el ciclo de vida de seguridad. Si hay una falla de algún elemento, se deben dar las razones de la falla, registrarse y corregirse.

8.8.1.3 Aceptación final del SIS. El objetivo de esta etapa es que el contratista en conjunto con Pemex verifique a través de inspección y pruebas, que el SIS fue construido, instalado y comisionado de acuerdo a los requerimientos de las especificaciones de diseño y que se encuentra listo para operar, para lo cual debe realizarse el acta correspondiente.

El contratista debe generar y entregar los informes de la prueba integral del SIS, indicando los resultados de las pruebas, si se cumplieron los objetivos y los criterios identificados durante la fase del diseño.

La documentación para la aceptación final del SIS debe estar actualizada. El contratista debe suministrar toda la documentación generada en todas las etapas del proyecto, el manual de operación y la información técnica en idioma y las unidades de acuerdo a lo que establece la Ley Federal sobre Metrología y Normalización y su reglamento.

La documentación requerida para soportar la prueba integral y que forma parte del proceso de aceptación del SIS debe incluir los siguientes puntos:

a) La descripción global del sistema.
b) Especificación funcional del sistema.
c) Diagramas de configuración completa del sistema.
d) Manual de usuario y licencias del software de usuario.
e) Protocolos, informes y actas de aceptación de pruebas en fábrica PAF (FAT) y en sitio (PAS, OSAT).
f) Procedimientos, informe y acta de aceptación de las pruebas integrales.
g) Copia de la especificación de los requerimientos de diseño.
h) Listado impreso del programa del procesador lógico.
i) Un diagrama de bloques del sistema global.
j) Una lista completa de las entradas/salidas.
k) Diagramas de proceso e instrumentación.
l) Índice de instrumentos.
m) Diagramas de lazos.
n) Esquemas eléctricos.
o) Matriz de Paro de Emergencia.
p) Planos que indiquen la localización de los equipos principales (PLG).
q) Diagramas de conexiones en gabinetes, diagramas que indiquen la interconexión y las terminales de todos los cables, diagramas unifilares eléctricos.
r) Diagramas de tubings del sistema neumático.
s) Documentación del proveedor del equipo, incluyendo especificaciones, requerimientos de instalación, y manuales de operación.
t) Pruebas de desempeño.

La aceptación final del SIS se debe realizar después de que el contratista haya demostrado a Pemex que el SIS opera con los demás componentes de la instalación interrelacionados con dicho SIS y entregue la documentación anterior.

8.8.1.4 Requerimientos de capacitación. El diseñador/licenciador del sistema junto con personal de Pemex deben identificar el nivel de entrenamiento, de entendimiento y documentación adicionales necesarios para que el personal de operación, instrumentación y de mantenimiento operen y mantengan de manera efectiva el sistema instrumentado de seguridad. Se deben impartir los siguientes cursos:

a) Curso de configuración de:
   - Interfase humano-máquina (IHM).
   - Procesador lógico.
b) Cursos de operación y mantenimiento del Sistema Instrumentado de Seguridad (SIS). Dichos cursos deben considerar los siguientes temas: filosofía de operación, mantenimiento preventivo, predictivo y pruebas de diagnóstico del SIS, interpretación de fallas y diagnósticos, instalación y operación del software de control, supervisión y alarmas, arranque y puesta en servicio del sistema.

Por lo tanto el contratista debe dar la capacitación y efectuar la evaluación del personal que opere el SIS. La capacitación a la que sean sometidos los operadores debe definir los siguientes puntos:

a) Cómo se llevan a cabo las funciones del SIS (puntos de disparo y las acciones que toma el SIS al verse rebasados dichos puntos de disparo).
b) Los riesgos contra los cuales protege el SIS.
c) La operación y consecuencias en la operación de todos los desvíos (bypass) y bajo que circunstancias específicas deben ser aplicados dichos desvíos.
d) La operación de cualquier disparo manual y cuando específicamente deben realizarse dichos disparos.
e) Su comportamiento y acciones a tomar durante la activación de cualquier alarma.
f) La capacidad de programación o configuración del SIS.
g) La aplicación de la lógica del SIS.
h) Un entendimiento de los requerimientos operacionales del sistema tanto desde la perspectiva del(os) operador(es) como desde la perspectiva del(os) ingeniero(s) a cargo del SIS.
i) Un entendimiento de los estándares y normas existentes a la fecha referidos al uso de SIS, incluyendo a esta norma.

8.8.1.5 Pruebas funcionales en línea. Para todas aquellas aplicaciones en las cuales no sea práctico o sea difícil llevar a cabo pruebas funcionales fuera de línea, el contratista debe proporcionar procedimientos para llevar a cabo pruebas funcionales en línea. Dichos procedimientos deben incluir:

a) Pruebas funcionales al elemento final durante los paros programados a la unidad.
b) Probar las salidas hasta dónde sea posible.

Para el caso de válvulas, la pruebas de movimiento parcial reducen la necesidad de pruebas funcionales completas, el contratista debe indicar en los procedimientos los periodos de tiempo mínimo en los cuales se deban llevar a cabo pruebas totales.

8.8.2 Operación y mantenimiento del SIS.

El principal objetivo de la operación y mantenimiento del SIS es asegurar que será operado y mantenido dentro de las especificaciones de integridad de seguridad requerida, garantizando que el SIL (NIS) de cada función de seguridad se mantiene dentro de los límites. El mantenimiento se debe centrar en asegurar que el sistema no se deteriore y que no llegue a tener un nivel de integridad por debajo de lo especificado.

8.8.2.1 Requerimientos. El contratista debe realizar la planeación de las actividades de operación y mantenimiento durante la etapa de diseño, antes de que el SIS sea puesto en operación. Esta actividad debe incluir los siguientes factores:

a) Descripción general del SIS.
b) Actividades para operación rutinaria y anormal.
c) Pruebas funcionales.
d) Actividades de mantenimiento preventivo y correctivo.
e) Identificar y controlar cualquier actividad que anule el SIS
f) Los procedimientos, medidas y técnicas a emplear durante la operación y mantenimiento.
g) Cuándo se deben llevar a cabo las actividades.
h) Equipos y herramientas necesarias para llevar a cabo las actividades.
i) Las personas, departamentos y organizaciones que se responsabilizaran de las actividades.
j) El grado de capacitación y competencia requerido por el ó los equipos que deben llevar a cabo las actividades de operación y/o mantenimiento.
k) Especificación del tipo de información de confiabilidad que debe recopilarse y analizarse durante la fase operativa.
l) Límites de operación segura y las implicaciones de seguridad si éstos son excedidos.
m) Tiempo requerido por las funciones del SIS incluyendo a los dispositivos de salida.
n) Especificaciones de desempeño.
o) Diagramas del SIS.
p) La matriz de paro de emergencia.

8.8.2.2 Procedimientos de operación y mantenimiento. Los procedimientos operativos y de mantenimiento deben ser desarrollados por el contratista tomando en cuenta los requerimientos antes citados a fin de asegurar que el SIS realizará sus funciones de acuerdo con los requerimientos de diseño. Dichos procedimientos deben ser:

a) Procedimientos de acciones rutinarias necesarias para mantener la seguridad funcional requerida del SIS.
b) Procedimientos de cómo llevará el SIS al proceso a un estado seguro.
c) Procedimientos del uso correcto de desvíos operativos o de mantenimiento (bypass), permisivos, restablecimientos del sistema, entre otros, a fin de prevenir estados inseguros o reducir las consecuencias de un evento peligroso.
d) Procedimientos de respuestas a alarmas o disparos del SIS
e) Procedimientos de mantenimiento que deben seguirse cuando ocurren fallas en el SIS.
f) Procedimientos para seguir el desempeño del mantenimiento.
g) Procedimientos para seguir la activación y fallas del SIS.
h) Procedimientos que aseguren que los equipos empleados en las pruebas y el mantenimiento están correctamente calibrados.
i) Procedimientos de administración de cambios durante la operación.

8.8.2.3 Procedimientos de administración de cambios durante la operación.

Plan de Mantenimiento. El contratista debe establecer y entregar los programas de mantenimiento, en lo cuales se detalle de manera escrita procedimientos de mantenimiento, pruebas y reparación del SIS a fin de mantener el nivel de integridad de seguridad requerido. El programa de mantenimiento debe diseñarse de tal forma que permita revelar lo que el SIS no detecte automáticamente.

La confiabilidad global del sistema debe considerar la no-disponibilidad durante las pruebas así como los tiempos medios de reparación.

El plan de mantenimiento del SIS debe incluir:

a) Programas periódicos de pruebas funcionales del SIS.
b) Inspecciones regulares a los equipos de campo para detectar cualquier deterioro visible.
c) Programas periódicos de mantenimiento preventivo a los sistemas que lo requieran.
d) Reparación de fallas detectadas. Una vez terminadas las reparaciones se deben realizar las pruebas apropiadas.

8.8.2.4 Modificaciones durante la operación del SIS. Esta etapa consiste en asegurar que al contratar cualquier tipo de cambio al SIS se realice de manera planeada y aprobada por Pemex. Así mismo, el control del cambio debe garantizar que el nivel de integridad de seguridad requerido no se vea comprometido.

El contratista debe aplicar el procedimiento de administración de cambios proporcionado por Pemex. El contratista debe asegurar que antes de realizar cualquier cambio se:

a) Modificaran los procedimientos operativos pertinentes.
b) Tiene definido el programa correspondiente.
c) Cuenta con la autorización y aprobación necesaria.
d) Han evaluado y comparado los riesgos involucrados si el cambio se lleva a cabo en línea o fuera de línea.
e) Garantiza que el nivel de integridad de seguridad no se vea comprometido.

Dependiendo de la magnitud del cambio se debe repetir el ciclo de vida de seguridad a partir de aquella fase que se vea afectada por el cambio.

Cuando se realicen cambios al software, éste debe ser probado exhaustivamente antes de su implantación, además el contratista debe proporcionar un procedimiento que permita el retorno automático del sistema a la versión anterior del software en caso de que se detecte alguna falla en el software.

El contratista debe evaluar el impacto en la integridad global del sistema de cualquier cambio en las condiciones ambientales tales como: temperatura, presión, humedad, vibración, disturbios electromagnéticos, entre otros.

8.8.2.4.1 Documentación. Todos los cambios a los procedimientos operativos, información de seguridad del proceso, y documentación general del SIS deben verificarse y actualizarse antes de volver a poner en operación al SIS.

Toda la documentación debe protegerse adecuadamente contra destrucción, pérdida o modificación no autorizada.

8.8.2.5 Consideraciones para la operación y mantenimiento en instalaciones rentadas. Todas las actividades relacionadas con la operación del SIS deben llevarse a cabo por personal que ha sido capacitado y evaluado.

Los operadores deben ser capacitados periódicamente, la periodicidad de la capacitación estará en función de: la actualización o cambios que sufra el SIS o alguno de sus componentes, la asignación o reasignación de operadores al SIS o se detecte que el operador no comprende algún punto relacionado con el SIS o alguno de sus componentes.

En la operación y mantenimiento deben monitorearse y registrarse:

a) Acciones que toma el SIS después de una demanda.

b) Fallas en los equipos que conforman el SIS. para actuar en demanda
c) Fallas que se encuentren en los equipos que componen el SIS durante las pruebas de rutina.
d) Causas de las demandas.
e) La frecuencia de las demandas, verificar que esta frecuencia concuerde con la frecuencia de demanda supuesta en el diseño.

En los casos donde sea necesario reemplazar componentes que fallen o se dañen, el reemplazo preferentemente debe hacerse con unidades idénticas que tengan exactamente las mismas especificaciones de confiabilidad. En caso de que un componente del SIS sea reemplazado por un componente con características diferentes, el cambio se debe considerar como una modificación al SIS.

El SIS debe ser probado cada cierto intervalo de tiempo, dicho intervalo debe estar en función de la especificación de los requerimientos de seguridad (ver punto 8.4.5).

El personal responsable de la operación y mantenimiento debe aplicar los procedimientos de pruebas funcionales proporcionados por el contratista.

Debe seguirse el procedimiento de administración de cambios en los siguientes casos:

a) Reemplazo de un(os) componente(s) por otro(s) con diferentes características.
b) Cambios en los periodos de pruebas o los procedimientos para realizar éstas.
c) Cambios en los puntos de disparo debido a cambio en las condiciones de operación.
d) Cambios en los procedimientos de operación.
e) Surjan nuevas leyes en materia de seguridad o las ya existentes sean modificadas.
f) Se modifiquen las condiciones de proceso.
g) Cambios en los requerimientos de seguridad de la planta.
h) Cualquier cambio cuyo propósito sea la corrección de fallas sistemáticas.
i) Cambios debido a tasas de fallas más altas de las esperadas o deseadas.
j) Incrementos en la tasa de demanda del SIS.

Todo el personal involucrado con el sistema instrumentado de seguridad debe tener un conocimiento mínimo de lo citado en el punto de capacitación.

El contratista debe documentar el entrenamiento, experiencia y aptitudes de todo el personal involucrado en un SIS o en cualquier actividad del ciclo de vida del SIS.

El contratista deberá entregar los programas de pruebas funcionales y mantenimiento, así como la evidencia de que estos se están llevando a cabo.

8.9 Desmantelamiento del SIS.

Esta etapa consiste en asegurar que al contratar el desmantelamiento de cualquier SIS en servicio activo, debe hacerse bajo una supervisión con la conducción y autorización por parte de Pemex. En caso del desmantelamiento parcial del SIS se debe asegurar que el SIS remanente permanezca con las funciones durante y después del desmantelamiento parcial o disposición del equipo bajo control.

8.9.1 Requerimientos. El contratista debe realizar una reevaluación en la seguridad funcional como resultado de la actividad propuesta del desmantelamiento. Dicha reevaluación debe incluir una actualización del Análisis de riesgo suficiente para determinar el alcance y la profundidad que las fases subsecuentes del ciclo de vida de seguridad que necesite ser retomadas. La reevaluación debe considerar:

a) La seguridad funcional durante la ejecución de las actividades del desmantelamiento.
b) El impacto del desmantelamiento de un SIS en las unidades adyacentes de operación y servicios auxiliares.
c) Los resultados descritos en el punto 8.9.2.1 se deben documentar.
d) Antes de desmantelar o disponer del sistema el contratista debe preparar y entregar a aprobación de Pemex el plan que incluya los siguientes procedimientos:
   - El cierre de los sistemas relacionados con la seguridad que no estén activos E/E/PE.
   - Desmantelamiento de los sistemas relacionados con la seguridad E/E/PE.

Si alguna actividad de desmantelamiento o disposición tiene un impacto en la seguridad funcional de cualquier sistema relacionado con la seguridad, esto iniciara un retorno a la fase apropiada del ciclo de vida del SIS. Todas las fases subsecuentes se llevarán a cabo entonces de acuerdo con lo especificado en esta norma para el nivel de integridad de seguridad del SIS.

9. RESPONSABILIDADES.

9.1 Petróleos Mexicanos, Organismos Subsidiarios y Empresas Filiales.

Vigilar la aplicación de los requisitos y especificaciones de esta norma, en las actividades que se lleven a cabo en la determinación del nivel de integridad de seguridad para los sistemas instrumentados de seguridad en los procesos industriales de las instalaciones de Pemex.

9.2 Subcomité Técnico de Normalización.

Promover el conocimiento de esta norma entre las áreas usuarias Pemex, prestadores de servicios y contratistas, involucradas en él o los procesos técnicos y administrativos generados por la necesidad de efectuar estudios para determinar el NIS (SIL) y SIS.

9.3 Área usuaria de Pemex.

Aplicar la Ley de Obras Públicas y Servicios Relacionados con las Mismas, así como la Ley Federal de Metrología y Normalización, la Ley de adquisiciones, arrendamientos y servicios del sector público, en lo referente a adquirir, arrendar o contratar bienes y servicios.

9.4 Contratistas y/o prestadores de servicio.

Cumplir con los requerimientos especificados en esta norma.

9.5 Responsabilidad de Pemex con respecto al análisis de riesgo.

Pemex deberá proporcionar información lo más actualizada posible de sus instalaciones para desarrollar el análisis de riesgo necesario para la determinación del NIS (SIL) objetivo del Sistema Instrumentado de Seguridad. En caso de que se cuente con el análisis de riesgo de la instalación vigente en un período de 5 años, deberá ser proporcionado al contratista, para actualizarlo o complementarlo.

10. CONCORDANCIA CON NORMAS MEXICANAS O INTERNACIONALES.

Las siguientes documentos aplican parcialmente en esta norma de referencia.

10.1 IEC 61508, 2000 Estándar Seguridad Funcional: Sistemas de Seguridad (Functional Safety: Safety Related Systems, IEC Standard 61508, 2000).

10.2 ISO 11064-3, Diseño Ergonómico de Centros de Control, Parte 3, Cuarto de Control, Primera Edición, 02/01/2002 (Ergonomic Design of Control Centres, Part 3: Control Room Layout, First Edition, Technical Corrigendum 1: 02/01/2002.

10.3 ISO 9000-3, Administración de la Calidad y Estándares de Aseguramiento de la Calidad, Parte 3: Guías para la aplicación de ISO 9001-1994 para el desarrollo, suministro, instalación y mantenimiento de los programas de cómputo, 2° Edición (Quality Management and Quality Assurance Standards, Part 3: Guidelines for the Application of ISO 9001-1994 to the Development, Supply, Installation and Maintenance of Computer Software, Second Edition).

10.4 IEC 870-5-5, Sistemas y Equipo de Control a Distancia, Parte 5: Protocolos de Transmisión, Sección 5, Funciones de aplicación básica, subinciso 6.1: Inicialización de la estación, 1°Edición 1996 (Telecontrol Equipment and Systems, Part 5, Transmission Protocols, Fisrts Edition, 1996)

10.5 IEC 60534-2, Válvulas de Control de Procesos Industriales, Parte 2: Capacidad de flujo, Septiembre 1998 (Industrial Process Control Valves, Part 2: Flow Capacity, September 1998).

10.6 IEC 61131-2 Controladores Programables 1994, Parte 2, Requerimientos de pruebas del equipo. (IEC 61131-2 Programmable Controllers 1994, Part 2).

10.7 IEC 801-2, Descarga Electrostática Nivel 3 (Level 3, Electrostatic Discharge).

10.8 IEC-61131-3 Controladores Programables 1994, Parte 3, Lenguajes de programación (IEC 61131-3 Programmable Controllers 1994, Part 2).

11 BIBLIOGRAFIA.

11.1 Análisis de capas de protección y procesos inherentemente más seguros. Arthur M. (Art) Dowell, III. Process Safety Progress, Vol 18, No. 4, Invierno 1999. (Layer of Protection Analysis and Inherently Safer Processes. Arthur M. (Art) Dowell, III. Process Safety Progress, Vol 18, No. 4, Winter 1999).

11.2 ANSI/ISA-S7.3-1981 (R1981), Estándares de calidad para el aire de instrumentos, Sociedad Instrumentista de América, 1981. (Quality Standard for Instrument Air, Instrument Society of America, 1981).

11.3 ANSI/ISA-S7.4-1981. Presiones de aire para controladores neumáticos, transmisores y sistemas de transmisión, Sociedad Instrumentista de América, 1983. (Air Pressures for Pneumatic Controllers, Transmitters and Transmission Systems, Instrument Society of America, 1983.

11.4 ANSI/FCI 70-2, Estándar de control de calidad para fugas de asiento en válvulas de control (Quality Control Standard for Control Valve Seat Leakage)

11.5 API RP552, Octubre 1994 Sistemas de Transmisión (API RP552, October 1994, Transmission Systems).

11.6 API 553, Primera Edición Septiembre 1998, Válvulas de control en refinerías (API 553 First Edition September 1998, Refinery Control Valves)

11.7 API Std 607, Pruebas de fuego para válvulas de asiento ligero de un cuarto de vuelta (Fire Test for Soft-Seated Quarter-turn valves)

11.8 API Std 609, Válvulas de mariposa (Butterfly valves: doubled flanged Lug and Wafer type)

11.9 API Spec 6FA, Especificación para pruebas de fuego para válvulas (Specification for fire tests for valves)

11.10 API RP540, Instalaciones eléctricas en plantas de procesamiento de petróleo, 4° edición, abril de 1999. (Electrical Installations in Petroleum Processing Plants, Fourth Edition, April 1999).

11.11 API RP651, Protección catódica de tanques de almacenamiento de petróleo, 2° edición, noviembre de 1997 (Cathodic Protection of Aboveground Petroleum Storage Tanks, Second Edition, November 1, 1997).

11.12 Aplicación de los Sistemas Instrumentados de Seguridad para las industrias de proceso, Estándar ANSI/ISA S84.01-1996, 1996 (Application of Safety Instrumented Systems for the Process Industries, ANSI/ISA standard S84.01-1996, 1996).

11.13 Base de datos de confiabilidad costa fuera (OREDA), SINTEF, 1999. (Offshore Reliability Data Handbook (OREDA), SINTEF Industrial Management, 1999).

11.14 ASTM E 1884–97, Guía estándar para requerimientos generales para cuerpos de evaluación y certificación/registro de sistemas de calidad, Sociedad americana para pruebas y materiales. (Standard Guide for General Requirements for Bodies Operating Assessment and Certification/Registration of Quality Systems, American Society for Testing and Materials)

11.15 Guías para la automatización segura de procesos químicos, AIChE, 1993 (Guidelines for Safe Automation of Chemical Process, AIChE, 1993).

11.16 Guías para sistemas protectores basados en instrumentos, UKOOA, noviembre 1999, Num. 2 (Guidelines for Instrumented-Based Protective Systems, UKOOA, November 1999, Issues No 2).

11.17 IEEE C37.90.1 Pruebas de capacidad para soportar picos (SWC). (Surge Withstand Capability Tests).

11.18 IEEE 730-1998, Estándar para planes de aseguramiento de calidad del software. (Standard for Software Quality Assurance Plans)

11.19 IEEE 828-1998, Estándar para planes de administración de configuración de software. (Standard for Software Configuration Management Plans)

11.20 NACE RP0169, Control de corrosión externa sobre sistemas de tubería metálica enterradas o sumergidas, Junio 1996 (Control of external Corrosion on Underground or Submerged Metallic Piping Systems. June 1996).

11.21 NACE RP0176, Control de corrosión de plataformas costa fuera fijas de acero asociadas con la producción de petróleo, enero 1994 (Corrosion Control of Steel Fixed Offshore Platforms Associated with Petroleum Production, January 1994).

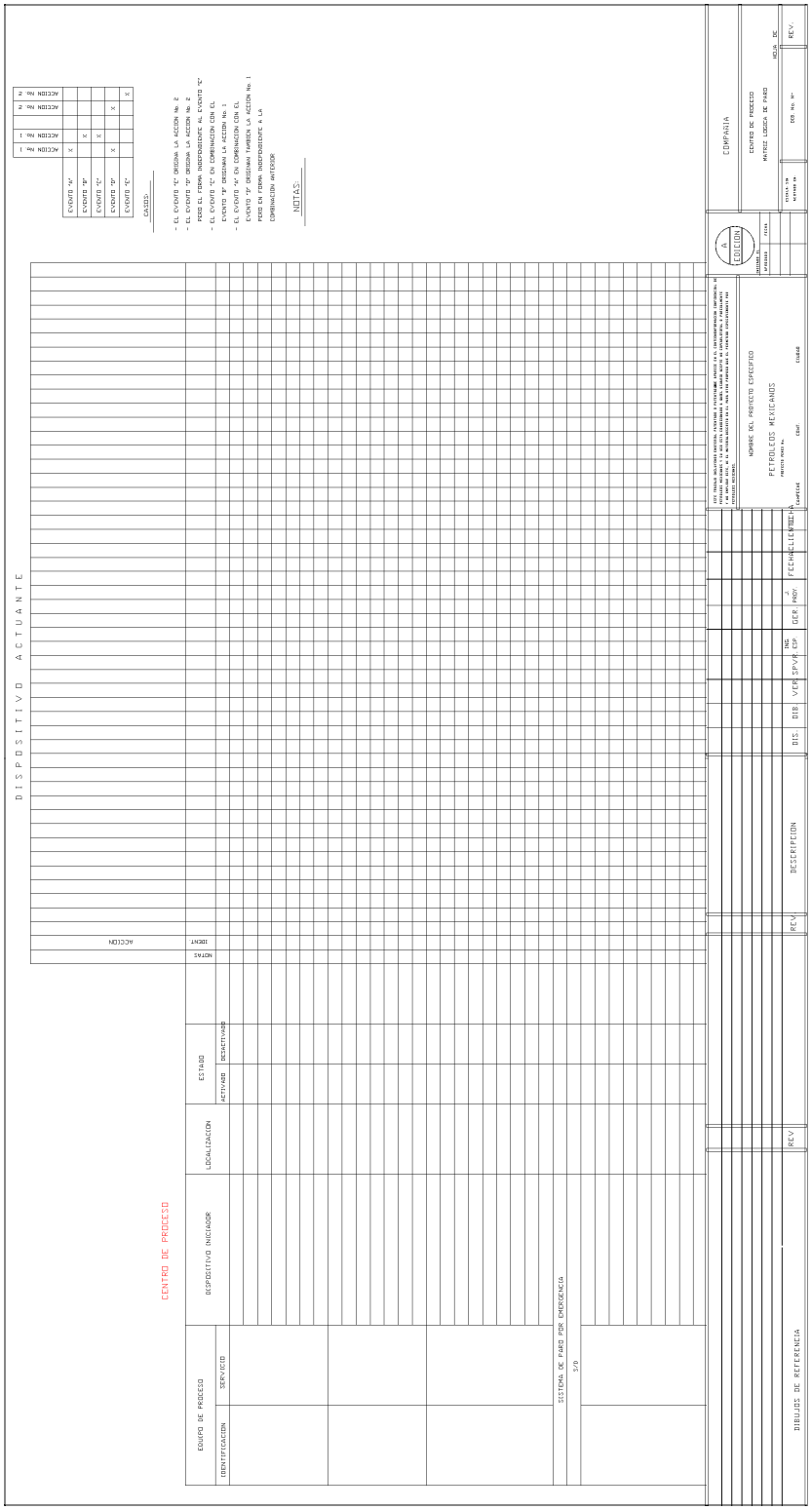
11.22 NACE RP0675, Control de corrosión externa sobre tuberías de acero inoxidable costa fuera (Control of External Corrosion on Offshore Steel Pipelines).

11.23 Sistemas de paro de seguridad: Diseño, Análisis y Justificación, Paul Gruhn y Harry L. Cheddie, ISA, 1998 (Safety Shutdown Systems: Design, Analysis and Justification, Paul Gruhn and Harry L. Cheddie, ISA, 1998).

11.24 Técnicas de Evaluación de los Niveles de Integridad de Seguridad (NIS) de Sistemas Instrumentados de Seguridad (SIS) ISA-TR84.0.02-1, 1998 (Safety Instrumented Systems (SIS) Safety Integrity Levels (NIS, SIL) Evaluation Techniques, ISA-TR84.0.02-1, 1998)

11.26 API Spec 6D “Especificación para válvulas en tuberías (compuerta, bloqueo, bola y check), 21° Edición, 31 de Marzo de 1994 (Specification for pipeline valves (gate, plug, ball and check), 21°Edition, March 31, 1994)

12. ANEXOS.



12.1 Anexo "A".1. Matriz lógica de paro para el sistema de paro de emergencia.